Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Access	is to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system or network.
Access control	is the prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
Access Control List (ACL)	are tables that tell a device operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program).
Account management	are the activities, techniques, and controls associated with establishing and changing user accounts, security classifications, and access rules related to IT resources in a systematic way.
Active Server Page (ASP)	is an HTML page that includes one or more scripts (small-embedded programs) that are processed on a Microsoft Web server before the page is sent to the user. An ASP is somewhat similar to a server-side include or a common gateway interface (CGI) application in that all involve programs that run on the server, usually tailoring a page for the user. Typically, the script in the Web page at the server uses input received as the result of the user's request for the page to access data from a database and then builds or customizes the page on the fly before sending it to the requestor.
Adabas	is a high-performance database for large, mission-critical applications. Adabas can be accessed via native calls from any development environment that is able to submit a call. Data is administered via SQL and standard interfaces such as ODBC or JDBC. Adabas is available on mainframe, Windows™ NT, and UNIX operating system platforms.
Adaptability	is the capability of a software application or product (hardware or software) to adjust fittingly to new requirements, conditions, and environments without requiring extensive modification.
Adaptive	is showing or having a capacity for or tendency toward adaptation, which is the adjustment or modification that makes something more fit given the conditions of its environment.
Advantage™	is Computer Associate's family of database management, application development, and enterprise reporting solutions that support on-going business operations, coupled with continued business growth. Given today's rapid expansion of business information and the need to consistently re-deploy this information throughout the enterprise, businesses must have solutions that minimize technology risk while maximizing return on technology investment. Advantage™ provides a broad range of proven production-worthy solutions that preserves the integrity of on-going business operations, providing a solid foundation that flexibly extends to embrace new business opportunities, enhancing return on investment for the overall IT infrastructure.
Adware	is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen..

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
American National Standards Institute (ANSI)	is a voluntary organization composed of corporate, government, and other members that coordinates standards-related activities, approves U.S. national standards, and develops positions for the United States in international standards organizations. ANSI helps develop international and United States standards relating to, among other things, communications and networking. ANSI is a member of the IEC and the ISO.
Anti-virus programs	are infection prevention programs that prevent the infection and replication process from occurring on computers, networks, operating, and communication systems.
Anti-virus software	is a class of program that searches a hard drive and floppy disks for any known or potential viruses. Also known as “anti-viral” software.
AppleTalk	is a routing protocol defined by Apple Computer, Inc., supporting data link access methods. AppleTalk runs over the 802.2 LLC portion of the LAN data link control layer.
Applets	are “little software programs.” Prior to the World Wide Web, the built-in writing, and drawing programs that came with Windows™ were known as "applets." On the Web, using Java™, an applet is a small software program that is sent along with a Web page to a user. Java™ applets can perform interactive animations, immediate calculations, or other simple tasks without having to send a user request back to the server.
Application	is a short expression for application program, a program designed to perform a specific function directly for the user or, in some cases, for another application program. Examples of software applications include office productivity, database programs, email, voice mail, customer relations management, Web browsers, software development tools, and communication programs. Applications use the services of the device’s operating system and of other supporting applications. An application program uses application program interfaces (API) as the means of communicating with other programs.
Application architecture perspectives: 3-tier client/server applications	are partitioned into three executable tiers of code: the user interface, the business rules, and the data access software. This does not mean that the three tiers execute on three different platforms. Often, the business-rule tier is deployed on the same platform as the data access tier, or on the same platform(s) as the user interface. 3-tier client/server applications can achieve higher performance efficiency by providing more flexibility in where application executables can be deployed as well as by making use of any available n-tier shared services. 3-tier client/server applications may be a good transition step from monolithic or two-tier applications.
Application architecture perspectives: Monolithic applications	, in which the programming code that implements the business rules, data access, and user interface are tightly coupled and integrated into a single, large software program. A monolithic application typically is deployed on a single platform, often a mainframe or midrange computer. The primary limitations of traditional monolithic applications include the absence of a browser presentation interface, interfaces to other applications, and the lack of component re-use to simplify modification and testing.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Application architecture perspectives: n-tier oriented application	n-tier oriented application architecture separates and distributes layers of logical functionality, often among three or more separate devices, in a distributed network. The most common form of n-tier (meaning 'some number of tiers') is the 3-tier application, in which user interface programming is in the user's client device, business logic is in a more centralized server device, and needed data is in a storage device that manages a database. In addition to the advantage of distributing programming and data throughout a network, n-tier applications can have any one tier executing on an appropriate device or operating system platform and be updated independently of the other tiers. Communication between the program tiers uses special program interfaces such as those provided by the Common Object Request Broker Architecture (CORBA). All n-tier applications regardless of development and deployment methodology share common structural layers of functionality, or tiers including the following: 1. #The presentation layer, comprised of interfaces, allows applications to communicate with users, other applications, and data resources. In n-tier oriented applications, the presentation layer is separated from the business rules so that changes in business rules do not require changes in interface programming, thereby decreasing the maintenance load, and allowing the development of a separate presentation interface. Recent extensions of wired/wireless devices (e.g., PDA's, telephony devices, Pocket PCs, etc.) emphasize the need for an independent presentation layer, separated from both application and platform. 2. Business rules define agency business processes and are the application implementation of policies and guidelines that an agency uses to accomplish its primary functions. As the business processes of agencies change, so must the business rules. Consequently, business applications should be constructed so that they can change, with as little disruption to current processes as possible. The business rules layer provides both the business algorithms that drive business processes and the knowledge of workflow and business events necessary to assemble a functional application. In n-tier-oriented applications, this tier consists of multiple callable objects or modules linked to each other and to the presentation and data access layers by message-based middleware. By separating business rules from the presentation and data access layer, the architecture simplifies maintenance, while maximizing flexibility and platform independence. 3. Data access mechanisms automate the storage, retrieval, and querying of data by software applications. Data access provides a critical interface between the application logic found in the business rules layer and the underlying file structures that store the physical data. In n-tier-oriented applications, middleware provides the interface between this layer and both the business-rule layer and the physical data. Middleware is a software infrastructure product, or suite of products, which provides links among the functional layers of an application. It also comprises the infrastructure components supporting the application. By separating the data access logic from the application logic, software architecture supplies additional flexibility and reuse opportunities not found in traditional application development.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Application architecture perspectives: Two-tier client/server applications applications	are constructed of software “clients” that, in order to perform their required function, must request assistance - “service” - from other software components known as “servers.” Middleware provides communication between the client and server. In two-tier client/server architecture, application functionality is partitioned into two executable parts, or “tiers.” 1. On one model, one tier contains the code that implements a graphical user interface (GUI) and the code that implements the business rules. This tier executes on PCs or workstations and requests data from the second application tier, which usually executes on the machine where the application’s data is stored. This model is referred to as two-tier, fat client. While the application has two tiers of executable code, most of the code is contained in the tier executing on the workstations - the “fat client.” Since business rules are tightly integrated with user interface code, the code that implements the business rules must be deployed on the same platform(s) as the user interface. 2. A second model for two-tier client/server applications has much of the code that implements the business rules tightly integrated with the data access code, sometimes in the form of database stored procedures and triggers. This model is called two-tier, fat server. Two-tier, fat server applications are often implemented as mainframe applications with Web browsers as user interfaces. This approach may be a useful first step to migrate to a 3-tier or n-tier, service-oriented application architecture. Users can enjoy the speed and ease-of-use provided by the web’s graphical interface while developers update other parts of the application.
Application benefit	is a quantified assessment of the benefits expected in the Budget Unit’s (BU) program and support areas by the information systems or telecommunication systems proposed. Application benefits can include reasonably projected reductions in program costs and increases in productivity of State personnel.
Application Program Interface (API)	is the means by which an application program talks to communications software. Standardized APIs allow application programs to be developed independently of the underlying method of communication. It comprises a set of standard software interrupts, calls, and data formats that computer application programs use to initiate contact with other devices (i.e., network services, mainframe communications programs, other program-to-program communications, etc.). Typically, APIs make it easier for software developers to create the links that an application needs to communicate with the operating system or with the network.
Application Service Providers (ASPs)	are companies that offer individuals or enterprises access over the Internet to applications and related services that would otherwise have to be located in their own personal or enterprise computers. Sometimes referred to as "apps-on-tap," ASP services are expected to become an important alternative, not only for smaller companies with low budgets for information technology, but also for larger companies as a form of outsourcing and for many services for individuals as well. Most corporations are essentially providing their own ASP service in-house, moving applications off personal computers, and putting them on a special kind of application server that is designed to handle the stripped-down kind of thin-client workstation. This allows an enterprise to reassert the central control over application cost and usage that corporations formerly had prior to the advent of the PC.
Application software	are the software programs that automate State and agency business functions, including tools that improve or enhance communications, the exchange of data, information, and resources, and productivity, etc.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Application Vulnerability Description Language (AVDL)	is a new security interoperability standard being proposed as an OASIS standard. AVDL creates a uniform way of describing application security vulnerabilities using XML. The XML-based technology will allow communication between products that find, block, fix, and report application security holes. Application security is a continuous lifecycle. Unfortunately, there is currently no standard way for these products to communicate with each other, making the overall security management process far too linear, manual, and time-consuming. A consistent definition of application security vulnerabilities is a significant step towards providing products that interoperate.
ArcGIS®	is a scalable system of software for geographic data creation, management, integration, analysis, and dissemination for every organization, from an individual to a globally distributed network of people. ArcGIS® embraces standards including geographic metadata standards (Federal Geographic Data Commission [FGDC]), Web standards (Extensible Markup Language [XML]), networking standards (TCP/IP), and the standard notation for the modeling of real-world objects (Unified Modeling Language [UML]). Users can deploy multiple ArcGIS® clients (ArcView®, ArcEditor®, and ArcInfo®.) ArcGIS® is a family of software products that form a complete GIS built on industry standards. ArcSDE® operates with commercial database management systems (DBMS), and it supports a variety of formats, including those from standards bodies such as the OpenGIS Consortium (OGC) and the International Organization for Standardization (ISO) as well as other vendors, such as the Oracle Spatial, Informix Spatial DataBlade, and IBM Spatial Extender formats. ArcView® provides data visualization, query, analysis, and integration capabilities along with the ability to create and edit simple geographic features.ArcEditor® includes all the functionality of ArcView® and adds the power to create and edit features in a multi-user, geo-database, or coverage. ArcInfo® includes all the functionality of ArcEditor® and adds advanced geoprocessing capabilities. Arc Macro Language (AML®) can be used to create ArcInfo® menus and macros. Avenue™ is ArcView's® GIS scripting language.
Arizona Portal Advisory Council (APAC)	is a board comprised of business and technology managers and directors from various areas of state and local government. APAC's purpose is to advise and make recommendations to the State CIO and the Portal Manager in the development, implementation, operation, and growth of the State's Web Portal – Arizona @ Your Service.
Assembler	is a device-specific programming language that takes basic computer instructions and converts them into a pattern of bits that the device's processor can use to perform its basic operations.
Assembly language	is a programming language that consists of instructions that are mnemonic codes for corresponding machine language instructions.
Asymmetric cryptography system	is an electronically processed algorithm or series of algorithms, which utilize two different keys with the following characteristics: 1.One key encrypts a given message; 2. One key decrypts a given message; and, 3. The keys have the property that makes it not feasible to discover one key from merely knowing the other key.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Asymmetric-key cryptography	is a cryptographic system that uses two keys, a public key known to everyone and a private or secret key known only to the recipient of the message. The public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.
Asynchronous	software program operation denotes that a process operates independently of other processes, whereas synchronous operation means that the process runs only because of some other process being completed or handing off operation.
Asynchronous Transfer Mode (ATM)	is an international standard for cell relay in which multiple service types (such as voice, video, or data) are conveyed in fixed-length (53 byte) cells. Fixed-length cells allow cell processing to occur in hardware, thereby reducing transit delays. ATM may be used in LAN and WAN communications.
Authentication	is the process of verifying the identity of an entity that is either providing or requesting resources, information, data, or documents.
Authentication, Authorization, and Accounting (AAA)	is a term for a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.
Authentication, data origin	is the service, when provided by the (N)-layer, provides corroboration to the (N+1)-entity that the source of the data is the claimed peer (N+1)-entity. The data origin authentication service provides the corroboration of the source of a data unit. The service does not provide protection against duplication or modification of data units.
Authentication, peer entity	is the service, when provided by the (N)-layer, provides corroboration to the (N+1)-entity is the claimed (N+1)-entity. This service is provided for use at the establishment of, or at times during, the data transfer phase of a connection to confirm the identities of one or more of the entities connected to one or more of the other entities. This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection.
Authorization	is the process of establishing and enforcing an entity's rights and privileges to access or provide specified resources, information, data, or documents.
Availabiliy	in the context of information security, refers to ensuring timely and reliable access to and use of information. The loss of availability is the disruption of access to or use of information or an information system. [44 U.S.C., Sec. 3542]
Backup	is a copy of information stored on non-volatile storage media used for restoring information in case of corruption, disaster, or sometimes for regulatory purposes.
Bandwidth	is the carrying capacity of a circuit, usually measured in bits per second for digital circuits or hertz for analog circuits.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
BASIC	was an early programming language that is still among the simplest and most popular of programming languages. Originally designed as an interactive mainframe timesharing language by John Kemeney and Thomas Kurtz in 1963, it became widely used on personal computers. BASIC continues to be widely used because it can be learned quickly, its statements are easy to read by other programmers, and support is available on most operating systems. BASIC's documentation has been translated into many national languages.
Biometrics	is unique, measurable physical or behavioral characteristics of a human being used for automatically recognizing or verifying identity. Biometric characteristics can include fingerprints, iris data, hand/face geometry, signature, voice, and DNA. Each of these methods has different degrees of accuracy, cost, social acceptability, and intrusiveness. An extreme example of an intrusive technique would be a DNA sample. Voice identification would be an example of a non-intrusive and socially acceptable technique.
Biometrics: face	geometry uses a standard video camera to capture facial images. The system extracts features that do not easily change, such as the geometry of the eyes and nose, from the images. The template created is matched against real-time images. People do change, and facial hair, positioning, and glasses can affect accuracy. Face geometry is less accurate than iris and fingerprint biometrics.
Biometrics: fingerprint	biometric are traditionally used as an identification tool in law enforcement. Fingerprint recognition systems convert a scanned image of a fingerprint into a mathematical representation of the features. The main strengths of fingerprint recognition are its long history, the variability inherent in fingerprints, ease of use, cost, and accuracy. Additionally, it has the potential to be integrated into inexpensive devices such as smart cards and keyboards. A disadvantage may be its social acceptability due to its negative association with illegal activities.
Biometrics: hand geometry	has features similar to fingerprints, though perhaps has higher social acceptability. Similar devices are used in both cases. Hand geometry is less accurate than fingerprints because of a lower number of features and less variability in the features. It may be acceptable when a user is matched against a known template. It would be less acceptable when trying to match against a large set of templates.
Biometrics: iris	biometrics uses the iris, which is the colored ring of tissue that surrounds the pupil of the eye. Iris identification is one of the most accurate biometric techniques because irises have more complex patterns and therefore more unique information available. It is generally more acceptable to users because a camera is used rather than the infrared beam used in retinal scans. Its advantages are in identifying individuals from a large set of choices. It is expensive because of the special optics required.

Keyword	Description
Biometrics: signature	verification depends on the rhythm, relative trajectories, speed, and number of pen touches in a signature. It measures the method of signing rather the appearance of the finished signature and so is different from the comparison of a signature. A pen-based computer or digitizing pad is required for signature capture during enrollment and during verification. It has a relatively low level of accuracy. It may be acceptable where a history of signature use exists, such as retail transactions and document authentication. It has limited uses where a large number of people must be identified in a limited time. It also has the disadvantage of requiring the individual to want to be identified. This limits its use in applications such as welfare or social-benefits-identification.
Biometrics: voice	biometrics is based on distinguishing the sound of a human voice based on the resonance of the vocal tract. It is different from voice recognition, which involves recognizing spoken commands or words. The system is trained by repeating a phrase that will be used as an access code. One shortcoming of voice biometrics is false rejects that deny a legitimate user access. This is due to medium-to-low accuracy rates and dependence on the type of equipment used. It may be suitable for outdoor situations and telephone access.
BizTalk	is an industry initiative to promote Extensible Markup Language (XML) as the common data exchange language for e-commerce and application integration on the Internet. While not a standards body per se, BizTalk is fostering a common XML message-passing architecture to tie systems together. BizTalk's premise is that the growth of e-commerce requires businesses using different computer technologies to have a means to share data. Accepting XML as a platform-neutral way to represent data transmitted between computers, BizTalk provides guidelines, referred to as the BizTalk Framework, for publishing schema (standard data structures) in XML and using XML messages to integrate software programs.
Block	is the unit of data in which information is stored and retrieved on storage devices such as disk drives and tapes.
Border Gateway Protocol (BGP)	based on IETF RFC1771, is a TCP/IP routing protocol for interdomain routing in large networks. It is used in the Internet and enables policy-based routing between ISPs. It could be applicable to corporate intranets that attach to the public Internet at more than one point. It is an alternative to EGP (Exterior Gateway Protocol). The current version is BGP-4.
Boundary router	is a router that performs packet filtering at the edge of a network to block certain attacks, filter unwanted protocols, and perform simple access control.
Bridge	is a device that connects and passes packets between two network segments that use the same communications protocol. Bridges operate at the data link layer (Layer 2) of the OSI reference model. In general, a bridge filters, forwards, or floods an incoming frame based on the MAC address of that frame.
Browser	is a GUI-based hypertext client application, such as Internet Explorer or Netscape Navigator, used to access hypertext documents and other services located on innumerable remote servers throughout the Internet and/or Intranets.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Btrieve	is a “Navigational” database engine. An application written in Btrieve can easily jump to the beginning or end of a table or traverse through it in an order defined by any number of key sequences. Btrieve also does not maintain information regarding the data it stores. The application passes an entire record of information for storage. Btrieve places the data into its file – sight unseen and with no validation. These are functions to be performed by the application. Even though Btrieve is “blind” to the data being stored, it does allow the application to define “keys” or “indexes” as a portion of the record that is being stored. These tell Btrieve how to sort the data. Btrieve has evolved into Pervasive.SQL.2000®.
Budget Unit (BU)	is a department, commission, board, institution or other agency of the State organization receiving, expending or disbursing State funds or incurring obligations of the State including the Board of Regents and the State Board of Directors for Community Colleges, but excluding the Universities under the jurisdiction of the Board of Regents and the Community Colleges under their respective jurisdictions and the Legislative or Judicial branches (ARS 41-3501(2)).
Building Industry Consulting Service International (BICSI)	is a not-for-profit telecommunications association that is a worldwide resource for technical publications, training, conferences, and registration programs for low-voltage cabling distribution design and installation.
Building Wiring System (BWS)	is a complete, operable data/video/voice communications physical wiring system within a building or between buildings in a campus environment.
Bus topology	describes the architecture for a linear network with the server(s) at one end and the client devices connected at various points along the network. A major disadvantage of bus architecture is that if one section goes down, a large portion of the network could be affected
Business Process Execution Language (BPEL)	for Web services is an XML-based language designed to enable task-sharing for a distributed computing or grid computing environment - even across multiple organizations - using a combination of Web services. Using BPEL, a programmer formally describes a business process that will take place across the Web in such a way that any cooperating entity can perform one or more steps in the process the same way.
C	is a structured, procedural programming language that has been widely used both for operating systems and applications and that has had a wide following in the academic community. Many versions of UNIX-based operating systems are written in C. C has been standardized as part of the Portable Operating System Interface (POSIX). With the increasing popularity of object-oriented programming (OOP), C is being rapidly replaced as "the" programming language by C++, a superset of the C language that uses an entirely different set of programming concepts, and by Java™, a language similar to but simpler than C++, that was designed for use in distributed networks.
C#	is a new object-oriented programming (OOP) language, which aims to combine the computing power of C++ with the programming ease of Visual Basic®. C# augments C++ and contains features similar to those of Java. C# simplifies programming through its use of Extensible Markup Language (XML) and Simple Object Access Protocol (SOAP), which allow access to a programming object or method without requiring the programmer to write additional code for each step.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
C++	is an object-oriented programming (OOP) language that is viewed by many as the best language for creating large-scale applications. C++ is a superset of the C language. A related programming language, Java™, is based on C++, but optimized for the distribution of program objects in a network such as the Internet.
Cabling	is the combination of all cables, jumpers, cords and connecting hardware used in a communications wiring system. Also known as Cabling System.
Calendar Access Protocol (CAP)	, currently an IETF Internet draft, specifies how a calendar interacts with a calendar store (CS) to manage calendar information. In particular, it specifies how to query, create, modify, and delete iCalendar components (e.g., events, to-dos, or daily journal entries). It further specifies how to search for available time information.
Calendaring and scheduling	products are well established for organizational use, but are usually limited to exchange of information among users of the same system, usually within the boundaries of a single organization. An IETF working group is pursuing development of standards to enable different products to interoperate and to work across organizational boundaries. This work will include the development of MIME content types to represent common objects needed for calendaring and scheduling transactions and access protocols between systems as well as between clients and servers. The working group will also consider and recommend solutions to the security issues concerning the exchange of calendar information between network entities. The Calendaring and Scheduling Working Group is chartered to focus on Internet standards for three basic problems facing group scheduling and calendaring users today. These include the following: 1. A standard content type for capturing calendar event and to-do information. The content type should be suitable as a MIME message entity that can be transferred over MIME-based email systems or HTTP World Wide Web. 2. A standard peer-to-peer protocol for common calendaring and group scheduling transactions. 3. A standard access protocol to allow for the management of calendars, events, and to-dos over the Internet.
Call Processing Language (CPL)	is an IETF Internet Draft, XML-based language that can be used to describe and control Internet telephony services. It is not tied to any particular signaling architecture or protocol; it is anticipated to be used with both the SIP and H.323. CPL is powerful enough to describe a large number of services and features, but it is limited enough in power so that it can run safely in Internet telephony servers.
Carrier Sense Multiple Access with Collision Detect (CSMA/CD)	is a media-access mechanism wherein devices ready to transmit data first check the channel for a carrier. If no carrier is sensed for a specific period, a device can transmit; however, if two devices transmit simultaneously, a collision occurs. This collision subsequently delays retransmissions from those devices for some random length of time. Ethernet and IEEE 802.3 use CSMA/CD access.
Carrier services	are telephone and data communications through some type of high-speed network channels to transport data between points in a Wide Area Network (WAN). Over time, as communications equipment becomes more sophisticated, the distinction between the types of traffic carried will cease.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Cascading Style Sheets (CSS)	is a Web page derived from multiple sources with a defined order of precedence where the definitions of any style element conflict. CSS is also a mechanism for adding style (e.g., fonts, colors, spacing, etc.) to Web documents. CSS level 1 (CSS1) describes the recommended approach for Web page designers and browser developers to adhere to. CSS level 2 (CSS2) builds on CSS1 and, with very few exceptions; all valid CSS1 style sheets are valid CSS2 style sheets. CSS2 supports media-specific style sheets so that authors may tailor the presentation of their documents to visual browsers, aural devices, printers, Braille devices, handheld devices, etc. This specification also supports content positioning, downloadable fonts, table layout, features for internationalization, automatic counters, and numbering, and some properties related to user interface. CSS level 3 (CSS3) is the modularization of the CSS specification. This modularization will help to clarify the relationships between the different parts of the specification and reduce the size of the complete document. The modular nature of the specification will make it possible for individual modules to be updated as needed, thus allowing for a more flexible and timely evolution of the specification as a whole.
Cascading Style Sheets Mobile Profile (CSSMP)	is a subset of CSS designed to accommodate mobile devices such as cellular telephones, PDA's, etc.
Category 5e	cabling is one of six grades of UTP cabling described in the EIA/TIA-568 standard. Category 5e cabling can transmit data at speeds of up to 1000 Mbps.
Category 6	cabling has been approved by the Telecommunications Industry Association (TIA) as TIA/EIA-568-B.2-1. This addendum is part of the TIA/EIA-568-B series of commercial building cabling standards. The new category 6 standard specifies requirements for 100-ohm balanced twisted-pair cables, connecting hardware, patch cords, channels and permanent links, and provides test procedures for laboratory and field performance verification over the frequency range of 1 to 250 MHz. Because category 6 supports positive power sum attenuation to crosstalk (PSACR) margins up to 200 MHz, this new cabling system offers double the bandwidth of category 5e cabling and vastly improved signal-to-noise margins. The category 6 standard also includes cable and connecting hardware balance recommendations for improved electromagnetic compatibility performance.
Cell	s the basic data unit for ATM switching and multiplexing. Cells contain identifiers that specify the data stream to which they belong. Each cell consists of a 5-byte header and 48 bytes of payload.
Cell relay	is a network technology based on the use of small, fixed-size packets, or cells. Because cells are fixed-length, they can be processed and switched in hardware at high speeds. Cell relay is the basis for many high-speed network protocols including ATM, IEEE 802.6, and Switched Multimegabit Data Service (SMDS).
Certificate of authority	is a security certificate that accompanies most software and OEM products. It contains anti-counterfeiting devices, such as a latent image to prevent the production of counterfeiting software products.
Certificate policy	is a formal document that describes the various roles involved in creating, maintaining, and validating digital certificates. It also specifies obligations associated with the roles and which parts of the process may be delegated.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Certification Authority (CA)	is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The role of the CA in this process is to guarantee that the individual granted the unique certificate, is in fact, who he/she claims to be.
Challenge Handshake Authentication Protocol (CHAP)	is a security feature supported on lines using Point-to-Point Protocol (PPP) encapsulation that prevents unauthorized access. CHAP does not itself prevent unauthorized access, but merely identifies the remote end. The router or access server then determines whether that user is allowed access.
Chief Information Officer for Information Technology (CIO-IT)	A. R. S. § 41-3503 establishes the Director of GITA as the CIO for Information Technology.
Cipher text	is encryption text. Plaintext is text before encryption, and cipher text is the encrypted result. The term cipher is also used as a synonym for cipher text.
Class of Service (CoS)	is a way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, streaming video, voice, large document file transfer) together and treating each type as a class with its own level of service priority. Unlike Quality of Service (QoS) traffic management, Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort."
Client/server	describes the relationship between two devices or applications in which one device or application, the client, makes a service request from another device or application, the server, which fulfills the request. Although the client/server model is used by applications within a single device, in a network, the client/server model provides a convenient way to interconnect devices or applications that are distributed efficiently across different locations. Also referred to as “two-tier application architecture.”
Clipper	is a complete application development system that is customized to fit real-life operational requirements. Clipper was a strategic Xbase development system for DOS developers.
Codec	is an acronym that stands for "compression/decompression." A codec is an algorithm, or specialized computer program, that reduces the number of bytes consumed by large files and programs. In order to minimize the amount of storage space required for a complicated file, such as a voice or video, compression is used. Compression works by eliminating redundancies in data. Compression can be done for any kind of file, including text, programs, images, audio, video, and virtual reality (VR). Compression can reduce the size of a file by a factor of 100 or more in some cases. For viewing, a decompression algorithm, which "undoes" the compression, would have to be used.
COM+	is an extension of Component Object Model (COM), Microsoft's strategic building block approach for developing application programs. COM+ is both an object-oriented programming architecture and a set of operating system services. It adds to COM a new set of system services for application components while they are running, such as notifying them of significant events or ensuring they are authorized to run.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Common Business Oriented Language (COBOL)	was the first widely used high-level programming language for business applications. COBOL was an effort to make a programming language that was like natural English, easy to write, and easier-to-read code. While COBOL has been updated over the years to combine COBOL programming with relational databases and the Internet, some factions in industry still perceive it as out-of-date and COBOL programs are generally viewed as legacy applications.
Common Data Security Architecture (CDSA)	is a set of layered security services and a cryptographic framework that provide an infrastructure for creating cross-platform, interoperable, security-enabled software applications for client-server environments. CDSA covers all the essential components of security capability, to equip software applications for electronic commerce and other business applications with security services that provide facilities for cryptography, certificate management, trust policy management, and key recovery. CDSA Version 2 is scalable such that it can provide security services for any device, ranging from Personal Digital Assistants (PDA) to mainframes, and any operating platform from Windows™ to UNIX / LINUX. Incorporating the CDSA solution into enterprise environments effectively decouples any single security solution from the infrastructure, and integrates a mechanism that allows plug and unplug security solutions as required.
Common Information Model (CIM)	is a computer-industry standard for defining device and application characteristics to allow system administrators and management programs to control devices and applications from different manufacturers or sources in the same way. CIM takes advantage of the Extensible Markup Language (XML); hardware and software makers choose one of several defined XML schemas (information structures) to supply CIM information about their product. CIM was developed by an industry group, the Distributed (formerly Desktop) Management Task Force (DMTF), as part of an initiative called Web-Based Enterprise Management (WBEM). CIM is intended to be more comprehensive than earlier models now in use, the Simple Network Management Protocol (SNMP) and Desktop Management Interface (DMI). With CIM, relationship information (what's connected to what) can be used to help trace the source and status of problems.
Common Internet File System (CIFS)	is the common file system used by the Microsoft® WindowsTM Operating System. The operating systems running on Microsoft® WindowsTM PCs do not include NFS. Instead, the protocol for remote file access is CIFS, formerly known as Server Message Block (SMB). In mid-1996, Microsoft® began to promote CIFS as an open standard with a published specification.
Common Object Request Broker Architecture (CORBA)	is an architecture and specification for creating, distributing, and managing distributed program objects in a network. CORBA allows applications at different locations to communicate in a network through an "interface broker." CORBA was developed by a consortium of vendors through the Object Management Group (OMG), to produce and maintain computer industry specifications for interoperable enterprise applications. Both International Organization for Standardization (ISO) and X/Open have sanctioned CORBA as the standard architecture for distributed objects (also known as components, which are reusable program building blocks that can be combined with other components in the same or other computers in a distributed network to form an application.) The CORBA specification defines the OMG's Object Management Architecture, ORB facilities, interfaces, and supplementary services.
Common Open Policy Service (COPS)	is a protocol for communicating network traffic policy information to network devices.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Common Warehouse Metamodel (CWM™)	is a specification that describes metadata interchange among data warehousing, business intelligence, knowledge management, and portal technologies. CWM provides a framework for representing metadata about data sources, data targets, transformation and analysis, and the processes and operations that create and manage warehouse data and provide lineage information about its use.
Communities of interest	are typically stakeholder groups, such as agencies, boards, and commissions with common interests in information, communication, or interaction. In the context of Security Architecture, a community of interest must establish an agreed upon rule set under which potential sharing of information and resources is sufficiently secure for all participants. In the context of Software and Data/Information Architecture, a community of interest has similar applications and data requirements, prompting initiatives that potentially cross over traditional agency boundaries.
Compilers	are special programs that process statements written in a particular programming language to transform the instructions into machine language or "code" that a device's processor uses. Typically, a programmer writes statements in a programming language such as COBOL or C. The file that is created contains what are called the source statements. The source statement file is executed using the appropriate compiler. When executing, the compiler first parses (or analyzes) all of the language statements syntactically one after the other and then, in one or more successive stages or "passes," builds the output code, making sure that statements that refer to other statements are referred to correctly in the final code. Traditionally, the output of the compilation has been called object code. (Note that the term "object" here is not related to object-oriented programming.) The object code is machine code that the processor can process or "execute" one instruction at a time.
Component Object Model (COM)	is Microsoft's framework for developing and supporting program component objects. It is aimed at providing similar capabilities to those defined in the Common Object Request Broker Architecture (CORBA), a framework for the interoperation of distributed objects in a network that is supported by other major companies in the computer industry.
Computer	is an electronic device that performs logic, arithmetic or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, software or communication facilities that are connected or related to such a device in a system or network.
Computer contaminant	is any set of computer instructions that is designed to modify, damage, destroy, record or transmit information within a computer, computer system or network without the intent or permission of the owner of the information, computer system or network. Computer contaminant includes a group of computer instructions, such as viruses or worms, that is self-replicating or self-propagating and that is designed to contaminate other computer programs or computer data, to consume computer resources, to modify, destroy, record or transmit data or in some other fashion to usurp the normal operation of the computer, computer system or network.
Computer program	is a series of instructions or statements, in a form acceptable to a computer that permits the functioning of a computer system in a manner designed to provide appropriate products from the computer system.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Computer services	includes computer time, data processing, storage functions and all types of communication functions.
Computer software	is a set of computer programs, procedures, and associated documentation concerned with the operation of a computer system.
Computer system	is a set of related, connected or unconnected computer equipment, devices and software, including storage, media and peripheral devices.
Confidentiality	in the context of information security, refers to preserving authorized restrictions of information access and disclosure, including means for protecting privacy and proprietary information. The loss of confidentiality is the unauthorized disclosure of information. [44 U.S.C., Sec. 3542]
Configuration management	is a management process for establishing and maintaining: (1) consistency of a product's performance, and (2) functional and physical attributes with its requirements, design, and operational information throughout the product's life.
Consultative Committee for International Telegraph and Telephone (CCITT)	is an international organization responsible for the development of communications standards, now called the ITU-T.
Control Language (CL)	allows system programmers and system administrators to write programs using operating system commands and other vendor-supplied commands.
Converged networks	use Internet Protocol to send data, voice, and video across a single network channel, which enables greater collaboration, simplifies network management, and reduces operating costs. Converged networks facilitate dynamic applications like e-learning, unified messaging, and integrated contact-center and customer-support systems. Historically, separate networks have been provisioned within the enterprise for data, voice, and video applications. These have often been deployed autonomously and operated in isolation, often implemented and managed by separate teams. These separate networks have been built to interconnect private branch exchange (PBX) equipment, H.320 videoconferencing equipment, and routers. The networks have been provisioned over dedicated leased lines for PBX and H.320 video, with a combination of leased lines, Frame-Relay, and ATM for data.
Copyright	is the right to make copies and/or the right to prohibit others from making copies according to Title 17 of the United States Code.
COTS	is an acronym for commercial-off-the-shelf application software, products purchased in the marketplace and installed without significant modification to interoperate with existing system components. The COTS approach avoids creating custom developed software.
Critical (or mission critical)	refers to those information resources whose unavailability or improper use has the potential to adversely affect the ability of an agency to accomplish its mission.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Cryptography	is a technology used to protect the confidentiality of information. Some forms of cryptography can also be the basis for ensuring the integrity of information and authentication of users. Cryptography uses algorithms to scramble (encrypt) and unscramble (decrypt) information such that only the holder of a cryptographic 'key' can encrypt or decrypt the information. A cryptographic 'key' is a string of alphanumeric characters used along with the information as input into a cryptographic algorithm.
Customer Information Control System (CICS)	is an online transaction processing (OLTP) program that, together with the COBOL programming language, has formed over the past several decades the most common set of tools for building customer transaction applications in large-enterprise, mainframe computing. A large number of the legacy applications still in use are COBOL/CICS applications.
Customer Premise Equipment (CPE)	, for the purposes of Arizona's EA, is any type of technology device (i.e., router, switch, firewall, server, PC, network appliance) that is installed at a customer site and is connected to the network infrastructure.
Data dictionaries	are a collection of descriptions of the data objects or items in a data model for the benefit of programmers and others who need to refer to them. A first step in analyzing a system of objects with which users interact is to identify each object and its relationship to other objects. This process is called data modeling and results in a picture of object relationships.
Data Encryption Standard (DES)	is a standard cryptographic algorithm developed by the U.S. National Institute of Standards and Technology (NIST).
Data integrity	is the assurance that information can only be accessed or modified by those authorized to do so. Data integrity can be maintained by the DBMS or maintained by the software application. Therefore, data integrity can be implemented inside the database and through data access rules. Data integrity includes the following: 1. Entity integrity keeps duplicate records from being inserted in a table and is enforced through primary keys and normalized database designs. 2. Domain integrity means that only valid values are entered into a field. It is enforced through foreign key constraints, column-level rules, or lookup tables. 3. Referential integrity makes sure that no foreign keys point to records that do not exist. It is enforced using foreign key constraints. 4. Business rules integrity applies additional rules to data as it specifically relates to the business. These rules may cross column, row, and even table or database boundaries.
Data marts	are subsets of a data warehouse. Where data warehouses are designed to support many requirements for multiple business needs, data marts are designed to support specific requirements for specific decision support applications (i.e., particular business needs). Although a data mart is a subset of a data warehouse, it is not necessarily smaller than a data warehouse. Specific decision support needs may still require large amounts of data. Data marts are typically considered a solution for distributed users who want exclusive control of the information required for their business need.
Data modeling	is the analysis of data objects that are used in a business or other context and the identification of the relationships among these data objects.

Keyword	Description
Data modeling, conceptual	is a high-level graphical representation of the data needed to operate an organization or a business activity that is unbiased toward any single application and independent of its access and physical storage. It is used to describe the information used by an organization in a business manner, which is not governed, by implementation-level issues and details.
Data modeling, logical	is a business perspective of a project's data that is independent of how it will be stored in the database. It describes the business data requirements in a format where business users can understand them.
Data modeling, physical	is a data model that directly represents the logical data, as it will be stored in the DBMS. The physical model is derived from the logical model.
Data models	provide a framework to collect and analyze data requirements and consist of entities, attributes, relationships, and cardinalities: 1. An entity is a person, place, thing, or concept and becomes a table in the database. A row in a table is an instance of an entity. 2. An attribute is a characteristic that provides further information about the entity like who, what, when, and where. It becomes a column in the database. A key attribute, or primary key, uniquely identifies an entity; so the values are distinct for each individual entity. 3. A relationship is how one entity is related to another. A relationship is shown through verbs or verb phrases because a relationship represents an action. 4. Cardinality is how many occurrences of an entity to expect in a relationship. There are two types of cardinality, conditional and unconditional. Conditional cardinality is where a relationship may or may not exist. The child entity is not required. Unconditional (mandatory) cardinality is where a relationship always exists.
Data warehouses	are a collection of data designed to support decision-making and analytical processing. Data warehouses contain a wide variety of data, usually from multiple data sources, presenting a comprehensive view of a particular business environment. Due to the nature of the data stored in a data warehouse, the size of the data warehouse is usually very large, so it requires special design and planning.
Database access middleware	provides software applications with the ability to access data stored in heterogeneous databases regardless of database management system and platform. The server-based middleware component, be it the DBMS server or gateway server, is responsible for mapping the SQL requests to the DBMS-specific SQL, interfacing to the DBMS system and marshalling the result sets for transmission back to the requestor. This includes data type conversions, caching of result sets, and packaging for transmittal. There are two forms of database middleware product: client-to-DBMS server and client-to-gateway server. Both of these use a client-side driver to facilitate cross-platform communication to the server. Applications interface to the driver via an Application Programming Interface (API).
Database Management System (DBMS)	is a set of computer programs with a user and/or programming interface that supports the definition of the format of a database, and the creation of and access to its data. A database management system removes the need for a user or program to manage low-level database storage. It also provides security for and assures the integrity of the data it contains. Types of database management systems are relational (table oriented) and object oriented.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Database software	is commonly referred to as the systems used to organize and manage data storage, facilitate access to, provide security for, and assure the integrity of data stored in a database.
Databases	are collections of information organized so that contents can easily be accessed, managed, and updated. The most prevalent type of database is the relational database, a tabular database in which data is defined so that it can be reorganized and accessed in a number of different ways. A distributed database is one that can be dispersed or replicated among different points in a network. An object-oriented programming database is one that is congruent with the data defined in object classes and subclasses.
DataFlex®	is an advanced, object-oriented 4GL designed for developing database applications. DataFlex is also a completely portable development environment. Applications can be developed under Windows™ Console Mode (98SE/NT/2000), Linux, and all leading UNIX systems.
Datagrams	are logical groupings of information sent as a network layer unit over a transmission medium without prior establishment of a virtual circuit. IP datagrams are the primary information units in the Internet. The terms cell, frame, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.
DataPerfect®	was an early PC DOS-based relational database program.
DB2®	is a relational database management system (RDBMS) available for a variety of platforms and operating systems. DB2® supports native XML functionality and integrates with other major RDBMS products. DB2® supports parallel architectures, integrated object models, industry standard SQL, Open Database Connectivity (ODBC) interface, the Java Database Connectivity™ (JDBC) interface, or a CORBA interface broker.
DBase® (II, III, IV)	were early PC-based relational database management systems (RDBMS) with application development tools.
DECnet	is the networking protocol used by Digital Equipment Corporation's Digital Network Architecture and is similar to the OSI 7 Layer Model with an additional network management layer.
Decryption	is the process of converting encrypted data back into its original form, so it can be understood.
Defense Data Network (DDN)	is the U.S. military network composed of an unclassified network (MILNET) and various secret and top-secret networks. DDN is operated and maintained by the Defense Information Systems Agency (DISA), formerly DCA. DISA is the U.S. military organization responsible for implementing and operating military information systems, including the DDN.
Delphi	is an object-oriented, visual programming approach to application development. Based on object Pascal programming language, the latest version of Delphi includes facilities for rapidly building or converting an application into a Web service. It provides interfaces for the programmer to build an application using the Extensible Markup Language (XML), Extensible Stylesheet Language (XSL), Simple Object Access Protocol (SOAP), and Web Services Description Language (WSDL).

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
DeMilitarized Zone (DMZ)	is a network created by connecting two firewalls that is added between a protected, trusted network and an external, untrusted network in order to provide an additional layer of security.
Desktop Management Interface (DMI)	is an industry framework for managing and keeping track of hardware and software components in a system of personal computers from a central location. DMI was created by the Desktop Management Task Force (DMTF) to automate system management and is particularly beneficial in a network computing environment where dozens or more computers are managed. DMI is hardware and operating system-independent, independent of specific management protocol, easy for vendors to adopt, mappable to existing management protocols such as Simple Network Management Protocol (SNMP), and used on network and non-network computers.
Desktop Managemewnt Task Force (DMTF)	is the industry organization that is leading the development, adoption and unification of management standards and initiatives for desktop, enterprise and Internet environments. Working with key technology vendors and affiliated standards groups, the DMTF is enabling a more integrated, cost-effective, and less crisis-driven approach to management through interoperable management solutions.
Development costs	are the sum of all start up costs such as vendor costs, vendor support costs, lease costs and other costs associated with the project.
Device	is a generic term for a server, storage, or client platform.
Device drivers	are programs that control devices that are directly attached to a platform. A device driver essentially converts the more general input/output (I/O) instructions of the operating system to messages that the device type can understand
Differentiated Services (DiffServ)	is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence - for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in terms of what is called Class of Service (CoS). Unlike the earlier mechanisms of 802.1p tagging and Type of Service (ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet.
Digital Subscriber Line (DSL)	is a public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are four types of DSL: ADSL, HDSL, SDSL, and VDSL. All are provisioned via modem pairs, with one modem located at a central office and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel.
Directory Access Protocol (DAP)	is a protocol used between a Directory User Agent (DUA) (software that accesses the X.500 Directory Service on behalf of the directory user) and a Directory System Agent (DSA) (software that provides the X.500 Directory Service for a portion of the directory information base) in an X.500 directory system.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Directory services	is 1. A method of integrating disparate sources of directory information into a single repository for use at the enterprise level. 2. the facility within networking software that provides access to, management of, and information about resources available on the network, including files, users, devices, data sources, applications, etc.
Directory Services Markup Language (DSML)	is an application of the Extensible Markup Language (XML) that enables different computer network directory formats to be expressed in a common format and shared by different directory systems. In the latest DSML specification, the related XML schema defines types of information found in today's network and enterprise directories. It then defines a common XML document format that should be used to display the contents of each directory. DSML is part of a handful of other efforts currently underway to adopt standards that make it easier for the contents of different directories to be shared across platforms and over the Internet. Other such efforts include the Directory Interoperability Forum and the Directory Enabled Networking (DEN) initiative. Proponents of DSML indicate that DSML also works synergistically with LDAP directories, allowing LDAP directory information to be transmitted beyond the traditional firewall and into Internet-based applications.
Directory Services Markup Language v1.0 (DSMLv1)	provides a means for representing directory structural information as an XML document. DSMLv2 goes further, providing a method for expressing directory queries and updates (and the results of these operations) as XML documents. DSMLv2 documents can be used in a variety of ways. DSMLv2 focuses on extending the reach of LDAP directories. Therefore, as in DSMLv1, the design approach is not to abstract the capabilities of LDAP directories as they exist today, but instead to faithfully represent LDAP directories in XML. The difference is that DSMLv1 represented the state of a directory while DSMLv2 represents the operations that an LDAP directory can perform and the results of such operations.
Directory-Enabled Networking (DEN)	is an industry-standard initiative and specification for how to construct and store information about a network's users, applications, and data in a central directory. A standard way of describing the network's elements in a central repository can enable applications to be developed that will automatically learn of user access privileges, bandwidth assignments, resource policies, and provide services accordingly. The result should reduce the cost of running the network and enable new services. DEN defines an object-oriented information model that is based on Common Information Model (CIM). Both models are being mapped into the directory defined as part of the Lightweight Directory Access Protocol (LDAP). DEN and CIM are an advancement, and can be used with Simple Network Management Protocol (SNMP).
Distributed Component Object Model (DCOM)	is a set of Microsoft® concepts and program interfaces in which client program objects can request services from server program objects on other computers in a network. DCOM is based on the Component Object Model (COM), which provides a set of interfaces allowing clients and servers to communicate within the same computer.
Distributed Computing Environment (DCE)	is a distributed programming architecture that preceded the trend toward object-oriented programming and CORBA, which is currently used by a number of large companies. DCE continues to exist along with CORBA with gateways or "bridges" between the two.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Document Object Model (DOM)	is a programming interface specification being developed by the World Wide Web Consortium (W3C), lets a programmer create and modify HTML pages and XML documents as full-fledged program objects. Currently, HTML (Hypertext Markup Language) and XML (Extensible Markup Language) are ways to express a document in terms of a data structure. As program objects, such documents will be able to have their contents and data "hidden" within the object, helping to ensure control over who can manipulate the document. As objects, documents can carry with them the object-oriented procedures called methods. DOM is a strategic and open effort to specify how to provide programming control over documents. It was inspired in part by the advent of the new HTML capabilities generally called dynamic HTML and as a way to encourage consistent browser behavior with Web pages and their elements.
Documented access	is system, application, and information access granted in accordance with a formal, written, and auditable process (including a formal, written request for access to specific systems or data).
Domain Name Services (DNS)	is a system used on the Internet for translating names of network nodes into addresses. DNS provides a centralized name service and can run over UDP or TCP.
Domain Specific Part (DSP)	is part of a Network Service Access Point (NSAP) format ATM address that contains an area identifier, a station identifier, and a selector byte.
Downloading	is the transmission of a file from one computer system to another, usually smaller computer system. From the Internet user's point-of-view, to download a file is to request it from another computer (or from a Web page on another computer) and to receive it.
Dynamic Content	is information that changes, or has the potential to change, each time a viewer accesses a web page. This type of content is usually generated from a database rather than coded directly into an HTML page. Generating the content requires programming and, typically, database support.
Dynamic Host Configuration Protocol (DHCP)	based on IETF RFC2131, is a protocol for dynamic IP address assignment and automatic TCP/IP configuration that provides both static and dynamic address allocation.
Easytrieve	is an information retrieval and data management tool designed to simplify programming. It serves as a powerful productivity language for business and information processing that provides easy-to-use information retrieval, sophisticated report writing, and comprehensive application development capabilities.
Electromagnetic Interference (EMI)	is the interference by electromagnetic signals that can cause reduced data integrity and increased error rates on transmission channels.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Electronic Business XML (ebXML)	is a project to use the Extensible Markup Language (XML) to standardize the secure exchange of business data. Among other purposes, ebXML would encompass and perhaps replace a familiar standard called Electronic Data Interchange (EDI). ebXML is designed to enable a global electronic marketplace in which enterprises can securely transact business through the exchange of XML-based messages. The United Nations body for Trade Facilitation and Electronic Business Information Standards (UN/CEFACT) and the Organization for the Advancement of Structured Information Standards (OASIS) launched the project as a joint initiative. Because ebXML relies on the Internet's existing standards such as HTTP, TCP/IP, MIME, SMTP, FTP, UML, and XML, it can be implemented and deployed on virtually any computing platform. The use of existing standards gives ebXML the advantage of being relatively inexpensive and easy to use.
Electronic Data Interchange (EDI)	is the electronic communication of operational data, such as orders and invoices, between organizations using a third-party value-added network or the Internet.
Electronic mail (e-mail)	is an electronic means for communication in which (a) usually text is transmitted, (b) operations include sending, storing, processing, and receiving information, (c) users are allowed to communicate under specific conditions, and (d) messages are held in storage unit called for by the addressee.
Emerging	is one of four categories used in the PSP program and EA to guide technology use in the State of Arizona (see also obsolescent, strategic, and transitional). “Emerging” implies that the State’s Enterprise Architecture promotes only evaluative deployments of this technology. This technology may be in development or may require evaluation in government and university settings.
Encryption	is the conversion of data into a form, called a cipher text, via electronic processing of a message so that the algorithm used to encode the message is infeasible to decipher without the corresponding decryption algorithm.
Encryption, asymmetric	is the method of electronically processing a message so that the algorithm used to encode the message is infeasible to decipher without the corresponding decryption algorithm.
Encryption, symmetric	is the method of electronically processing a message so that the same key is used to both encrypt and decrypt the message. DES and Triple DES are examples of symmetric encryption algorithms.
Enterprise Architecture (EA)	for the State of Arizona describes a comprehensive framework for information technology that supports the Arizona State government strategic plan. Enterprise Architecture includes important business, governance, and technical components. The technical components, collectively referred to as Enterprise Wide Technical Architecture (EWTA), provide technical guidance to State agencies. That guidance is supported by principles correlated to agency business functions, recommended standards, and applicable recommended best practices. Enterprise Architecture for the State of Arizona consists of five (5) domains: Security, Network, Platform, Software, and Data/Information.

Keyword	Description
Enterprise JavaBeans™ (EJB)	is an architecture for setting up program components, written in the Java™ programming language, that run in the server parts of a computer network in the client/server model. EJB™ offers enterprises the advantage of being able to control change at the server rather than having to update each individual computer with a client whenever a new program component is changed or added. EJB™ components have the advantage of being reusable in multiple applications.
Enterprise Storage Connection (ESCON)	is a 200 Mbps serial I/O bus used on IBM Corporation's Enterprise System 9000 data center computers. ESCON is similar to Fiber Channel in many respects, ESCON is based on redundant switches to which computers, and storage subsystems connect using serial optical connections.
Entity	refers to an individual or information system that has access to an information system or to its data, records, or documents.
ENUM	(RFC 2916) is the Internet Engineering Task Force (IETF) protocol that will assist in the convergence of the Public Switched Telephone Network (PSTN) and the IP network; it is the mapping of a telephone number from the PSTN to Internet services. ENUM was developed as a solution to the question of how to find services on the Internet using only a telephone number, and how telephones, which have an input mechanism limited to twelve keys on a keypad, can be used to access Internet services.
Ethernet	is a local area network (LAN) protocol that is specified in IEEE 802.3 and that uses Carrier Sense Multiple Access with Collision Detection (CMSA/CD), an OSI Level 2 media access method.
Exclusive rights	, There are five exclusive rights under Title 17 of the United States Code, Copyright Act. 1) the right to make copies, 2) the right to distribute copies to the public, 3) right to prepare derivative works, 4) the right to perform the work in public and 5) the right to display the work in public.
Extensible Hypertext Markup Language (XHTML)	is a family of current and future document types and modules that reproduce, subset, and extend HTML. XHTML document types are XML based, and ultimately are designed to work in conjunction with XML-based user agents.
eXtensible HyperText Markup Language Mobile Profile (XHTMLMP)	is a superset of XHTML Basic designed to accommodate mobile devices such as cellular telephones, PDA's, etc.. It includes all XHTML Basic modules plus some additional XHTML 1.0 tags.
Extensible Markup Language (XML)	is the universal format for structured documents and data on the Internet. XML is a set of rules (guidelines or conventions) for designing text formats to structure data. XML is extensible, platform-independent, and it supports internationalization and localization. XML and middleware are complimentary technologies. XML is intended for the storage and manipulation of text making up humane-readable documents like Web pages, while middleware solutions like CORBA tie cooperating computer applications exchanging transient data.
Extensible Markup Language Metadata Interchange Format (XMI)	is a model driven XML integration framework for defining, interchanging, manipulating, and integrating XML data and objects. XMI-based standards are in use for integrating tools, repositories, applications, and data warehouses. XMI specifies an open information interchange model that is intended to give developers working with object technology the ability to exchange programming data over the Internet in a standardized way, thus bringing consistency and compatibility to applications created in collaborative environments.

Keyword	Description
Extensible Stylesheet (XSL)	is a language for expressing style sheets. An XSL style sheet is, like with Cascading Style Sheets (CSS), a file that describes how to display an XML document of a given type. XSL shares the functionality of and is compatible with CSS2 (although it uses a different syntax). XSL adds a transformation language for XML documents: XSLT. Originally intended to perform complex styling operations, like the generation of tables of contents and indexes, it is now used as a general-purpose XML processing language. XSLT is widely used for purposes other than XSL, like generating HTML web pages from XML data.
Extensible Stylesheet Language Transformations (XSLT)	is a standard way to describe how to transform (change) the structure of an XML (Extensible Markup Language) document into an XML document having a different structure. XSLT is a recommendation of the World Wide Web Consortium (W3C). XSLT is an extension of the Extensible Stylesheet Language (XSL). XSL is a language for formatting an XML document (for example, showing how the data described in the XML document should be presented in a Web page). XSLT shows how the XML document should be reorganized into another data structure (which could then be presented by following an XSL style sheet.). XSLT is used to describe how to transform the source tree or data structure of an XML document into the result tree for a new XML document, which can be completely different in structure. The coding for the XSLT is also referred to as a style sheet and can be combined with an XSL style sheet or used independently.
External Environment Interface (EEI)	refers to the interfaces for external entities with which an application platform exchanges information, including the human end user, hardcopy documents, and physical devices. External Environment Interfaces provide primarily for interoperability.
Facilities issues	are concerns involving the physical locations of network-related equipment and wiring. Security of these assets becomes a major consideration as an increasing number of operations and resources become interconnected in a network-centric computing environment.
Fair competition	is the application of A.R.S. 41 § 2565 (part of the Arizona Procurement Code) to specifications for information technology hardware, software, and services in an effort to encourage competition in satisfying the State's needs while not being unduly restrictive.
Fault tolerance	is the ability for a system, device, or connection to continue operating after failure of any given component of the system, device, or connection.
Fiber Channel (FC)	is a high-speed interface technology nominally running at speeds of 1 Gbps. Data can be transmitted and received at one-gigabit-per-second simultaneously. Typically, the Small Computer System Interface (SCSI) runs over Fiber Channel, although Fiber Channel was designed to transport other protocols, too.
Fiber Channel over IP (FCIP)	is a proposed IETF standard, undergoing ratification in the IP storage-working group, to allow Fiber Channel frames to be encapsulated in IP so that both SCSI and non-SCSI frames can be transported transparently across an IP network.
Fiber Distributed Data Interface (FDDI)	is a LAN standard, defined by ANSI X3T9.5, specifying a 100 Mbps token-passing network using fiber-optic cable, with transmission distances of up to 200 km. FDDI uses dual-ring architecture to provide redundancy.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Fiber optics	is a transport medium for the transmission of information (audio, video, and data). Light is modulated and transmitted over high purity, hair-thin fibers of glass or plastic. The bandwidth capacity of fiber optic cable is much greater than that of conventional cable or copper wire.
File	is a data object that can be managed by a file system. Files act at an abstraction level that allows them to be given a symbolic name that uniquely identifies the data, which can be assigned ownership and access rights. Files may be created and deleted or may change in size during their lifetimes.
File infectors	are a second type of virus, which can attach themselves to executable files, such as files with the extension .COM, .EXE, .DLL, .OVR, or .OVL. When the file is executed, the virus, which operates in memory, spreads by attaching itself to other executable files. These types of viruses usually cause problems on LAN servers that run local applications shared by multiple systems. Unlike boot sector viruses, they can travel via a network as e-mail attachments or via file transfers. Gateway-based antivirus products stop the spread of these network-transported viruses by intercepting them at the network perimeter.
File Transfer Protocol (FTP)	is an application protocol, part of the TCP/IP protocol stack, used for transferring files between network nodes.
FileMaker® Pro	is a relational database application known for being easy to use and for its ability to serve Web pages dynamically without requiring the use of additional third-party applications. FileMaker® was originally developed as a personal database application for the Macintosh computer. In an effort to build upon FileMaker's® reputation for user friendliness, FileMaker® Pro has been purposely redesigned so that its user interface more closely resembles that of Microsoft's® office suite
Firewalls	are a common term for physical devices, software, and network architectures designed to block or filter access between a private network and a public network such as the Internet. Firewalls also provide access control between separate internal networks. Firewalls enforce the enterprise's security policy at determined perimeters, e.g., access point to the public Internet. To be effective, each must provide the single point of access to and from an un-trusted network.
Firewalls: application level	or proxy servers protect internal networks by not permitting direct access from the internal network to un-trusted networks such as the public Internet. Internal users connect to the `proxy', which then acts on their behalf, completing the connection to the requested external service. Proxy firewalls are specific to the applications they proxy. For example, a proxy for Web or FTP is installed to support those applications. Not all applications can be proxied. For those that cannot be proxied, proxy-like gateways shuttle data between internal and external networks. They maintain the characteristic of preventing direct connections between the internal and external networks.
Firewalls: packet-filtering	filter access at the packet level. By examining the contents of packets, they permit or deny access based on a defined access control policy. Packet filtering firewalls operate below the application and typically do not have access to information particular to an application.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Firewalls: stateful inspection	are packet filters that incorporate awareness of OSI Layer 4. Each time a TCP connection is established from an inside host accessing the Internet through the firewall, the information about the connection is logged in a stateful session flow table. The table contains the source and destination addresses, port numbers, TCP sequencing information, and additional flags for each TCP connection associated with that particular host. This information creates a connection object in the firewall. Thereafter, inbound packets are compared against session flows in the connection table and are permitted through the firewall only if an appropriate connection exists to validate their passage.
Flash memory	is constantly charged memory in which each bit of data is stored in a cell or transistor as one of two voltage levels. Flash memory is used to hold control code such as the Basic Input/Output System (BIOS) in a personal computer. When the BIOS needs to be changed (rewritten), the flash memory can be written to in block (rather than byte) sizes, making it easier to update.
Flat files	are files containing data records that have no structured interrelationship. The term is frequently used to describe a textual document from which all word processing or other structure characters or markup has been removed. In usage, there is some ambiguity about whether such markings as line breaks can be included in a "flat" file.
FORTRAN (FORmula TRANslation)	is a third-generation (3GL) programming language that was designed for use by engineers, mathematicians, and other users and creators of scientific algorithms. It has a very succinct and spartan syntax. Today, the C language has largely displaced FORTRAN.
Fourth (4th) Dimension (4D)	is a database and database development environment. 4D is a database product, comparable to Microsoft Access and Filemaker® Pro that is available for Macintosh™ operating systems and Windows™ operating systems.
FoxPro®	was a PC DOS/Windows™ based relational database management system (RDBMS) with application development tools. Its equivalent for the Macintosh platform was FoxBASE™. FoxPro® has evolved into Visual FoxPro®.
Frame	is the logical grouping of information sent as a data link layer unit over a transmission medium. A frame often refers to the header and the trailer, used for synchronization and error control, which surround the user data contained in the unit.
Frame relay	is an industry standard, switched, data-link-layer protocol that handles multiple virtual circuits using HDLC encapsulation between connected devices. It is a data communications interface, which provides high-speed transmission with minimum delay and efficient use of bandwidth. It does not have error detection or error control and it assumes that connections are reliable.
Gateways	are points (network point, device, software, etc.) that act as an entrance to another point (network, computer, software application, etc.).
General public license	is a public legal document whereby a licensee has agreed to read, understood and will comply with all terms and conditions for obtaining, using, copying, modifying and distributing software and/or documentation, usually without fee or royalty (a donation may be requested).

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Generic Security Service Application Program Interface (GSS-API)	defined in IETF RFC 1508 and 2078, provides security services to callers in a generic fashion, supportable with a range of underlying mechanisms and technologies and hence allowing source-level portability of applications to different environments.
Gigabit Ethernet	is a standard for a high-speed Ethernet that operates at one million bits per second. The standard for Gigabit Ethernet uses the same format as 10 Mbps and 100 Mbps Ethernet.
GOTS	is an acronym for government-off-the-shelf application software, products developed for a government agency with funding and specifications from the agency that is made available to other government agencies. GOTS also includes technology/system transfers from other government agencies. The GOTS approach avoids creating custom developed software.
Government Information Technology Agency (GITA)	is the Arizona State Government Executive Branch agency responsible for statewide information technology (IT) planning, coordination, and consulting. The Government Information Technology Agency (GITA) Director serves as the Chief Information Officer for State government. GITA has responsibility to administer the State's Executive Branch IT resources, including: establishing and maintaining statewide standards, serving as statewide coordinator, critically evaluating and approving/disapproving agency IT plans, approving/disapproving IT projects with development costs over $25,000, temporarily suspending the expenditure of monies if an IT project is at risk of failing to achieve its intended results or does not comply with State requirements, and ensuring IT compliance with statewide policy regarding accessibility to equipment and technology for citizens with disabilities. Legislation forming GITA was enacted in 1996 and implemented July 1, 1997.
Graphical User Interface (GUI)	is a user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored. Such conventions as buttons, icons, and windows are typical, and many actions are performed using a pointing device (such as a mouse).
Graphics Interchange Format (GIF)	is one of the two most common industry-wide file formats for graphic images on the Internet. The Unisys Corporation owns the compression algorithm used in the GIF format. IETF RFC 2083 defines the Portable Network Graphics (PNG) format specification as a patent-free replacement for the GIF.
Grid computing (or the use of a computational grid)	applies the resources of many computers in a network to a single problem at the same time - usually to a scientific or technical problem that requires a great number of computer processing cycles or access to large amounts of data. Grid computing requires the use of software that can divide and distribute pieces of a program to as many as several thousand computers. Grid computing can be thought of as distributed and large-scale cluster computing and as a form of network-distributed parallel processing. It can be confined to the network of computer workstations within a corporation or it can be a public collaboration (in which case it is also sometimes known as a form of peer-to-peer computing).

Keyword	Description
Groupware	refers to technologies and programs that help people work together collectively while located remotely from each other. Groupware services can include the sharing of calendars, collective writing, e-mail handling, shared database access, electronic meetings with each person able to see and display information to others, and other activities.
Guideline	is a best practice or an acceptable approach for implementing a policy or procedure. A guideline may become a standard.
H.320	is a suite of ITU-T standard specifications for videoconferencing over circuit-switched media, such as ISDN, fractional T1, and switched 56 Kbps lines. Extensions of ITU-T Standard H.320 enable videoconferencing over LANs and other packet-switched networks, as well as video over the Internet.
H.323	llows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of CODECs (integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals) call setup and negotiating procedures, and basic data transport methods.
Hardware platform	is the computer (device) and all of its non-software components.
Hierarchical databases	(also referred to as structured file systems) contain information structured in records that are subdivided into a hierarchy of related segments. Segments are further subdivided into fields. Information in the database records is subdivided into segments and fields on a logical basis, either by the inherent structure of the data or by consideration of the uses for the data.
High-Level Data Link Control (HDLC)	is an international protocol standard adopted by ISO for data link control implementations and forms the basis for ISDN and Frame Relay protocols.
Host-controlled devices	are client devices (computer terminals, traditional telephony instruments, etc.) that do not have an operating system associated with them. The interface of the device cannot be programmed and is limited to whatever functionality is provided by the host.
Hubs	are hardware or software devices that contain multiple independent but connected modules of network equipment. Hubs can be active (where they repeat signals sent through them) or passive (where they do not repeat, but merely split, signals sent through them).
Human Authentication API (HA-API)	is a generic API designed to allow a common set of instructions to integrate biometrics into applications requiring identification. The HA-API specification was prepared for the US DOD by the National Registry, Inc. Currently the Open Group is considering adopting the HA-API as part of common data security architecture.
Hypertext Markup Language (HTML)	is used for publishing hypertext on the Internet. It is a non-proprietary format based upon Standard Generalized Markup Language (SGML), and can be created and processed by a wide range of tools, from simple plain text editors to sophisticated What-You-See-Is-What-You-Get (WYSIWYG) authoring tools. HTML 4 is an SGML application conforming to ISO Standard 8879 and widely regarded as the standard publishing language of the Internet.

Keyword	Description
Hypertext Transfer Protocol (HTTP)	is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the Internet. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.
Hypertext Transfer Protocol over Secure Socket Layer (HTTPS)	is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is the use of SSL as a sub-layer under its regular HTTP application layering. HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.
Hyrid	in this domain document refers to a device that has two different types of components performing essentially the same function.
Ideal	is an advanced application development system that addresses all aspects of program creation and maintenance. It is used for prototyping and is closely integrated with Advantage™ CA-Datacom/DB Database™ and DB2®. It provides direct access to all tables and views as well as VSAM and sequential files, and supports programs that use SQL or its own highly efficient set/based constructs. SQL is embedded or generated by the compiler.
IDEF0	is a functional modeling method designed to model the decisions, actions, and activities of an organization or system. The IEEE 1320.1-1998 standard describes the ODEF0 functional modeling language (semantics and syntax) and associated rules and techniques for developing structured graphical representations of a system or enterprise. Use of this standard permits construction of models comprising system functions (activities, actions, processes, and operations), functional relationships, and data (information or objects). IDEF0 was derived from a well-established graphical language, the Structured Analysis and Design Technique (SADT). The United States Air Force commissioned the developers of SADT to develop a function modeling method for analyzing and communicating the functional perspective of a system. IDEF0 models help to organize the analysis of a system and to promote good communication between stakeholders.
IDEF1X	is a conceptual modeling method for designing relational databases with a syntax designed to support the semantic constructs necessary in developing a conceptual schema. The IEEE 1320.2-1998 standard describes the IDEF1X conceptual modeling language (semantics and syntax) and associated rules and techniques for developing a logical data model. Use of this standard permits construction of semantic data models that can support management of data as a resource, integration of software application systems, and building of databases. A conceptual schema is a single integrated definition of the enterprise data that is unbiased toward any single application and independent of its access and physical storage. Because it is a design method, IDEF1X is not particularly suited to serve as an AS-IS analysis tool. IDEF1X is most useful for logical database design after the information requirements are known and the decision to implement a relational database has been made. Hence, the IDEF1X system perspective is focused on the actual data elements in a relational database.
Identification	is the process of distinguishing one entity from all others. Identification techniques provide a means of gaining entry or access to resources, information, data, or documents.
IDMS	is a relational database management system (RDBMS) that provides support for ODBC and native JDBC drivers.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
IEEE 802.2	is a logical link control standard for local area networks (LANs). This standard of the Institute of Electrical and Electronics Engineers (IEEE) describes the function of the Logical Link Control (LLC) protocol used in both token ring and Ethernet LANs. 802.2 is one of a set of communications standards that define physical and electrical network connections. The 802.2 standard specifies the data link layer for use with 802.3 networks (thick, thin, twisted pair, and fiber-optic Ethernet networks) and with 802.5 networks (twisted pair or fiber-optic token ring networks).
IMS®	is a database management system organizes the data in different structures to optimize storage and retrieval, and ensure integrity and recovery. IMS is exploiting the latest programming technologies for the Internet and Java, including enabling of interactive and multimedia applications in a simplified fashion. IMS traditionally has supported a number of communications facilities. IMS has also provided interfaces for open Transaction and Database Management access to IMS applications/data from other subsystems using the latest technology. IMS provides connectivity and integration for leading edge end-to-end transaction integrity and real time data currency.
Indexed Sequential Access Method (ISAM)	is a file management system that allows data records to be accessed either sequentially (in the order they were entered) or randomly (with an index). Each index defines a different ordering of the records.
Industry de facto	refers to a condition being such in effect though not formally recognized. In these domain documents, industry de facto is used to indicate widely accepted and pervasive, although not formally accepted and endorsed by an official standards body.
Information assets	in the context of network security, information assets include the information technology infrastructure, applications, programs, databases and data elements that comprise them.
Information models	, also referred to as "meta-metadata," are components of data warehouse technology and typically document the following in a repository: 1. The business process driving the need for the data warehouse, 2. The data elements involved (and the associated metadata), 3. Relationships between data elements, 4. The flow of data into and out of the data warehouse, including the detailed processes that occur to input or output data in the data warehouse, 5. Business events affecting the data warehouse, and 6. Security requirements.
Information security	means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide – (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions from access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.
Information Services Inventory System (ISIS	is a web-based application, located at http://gita.state.az.us/apps, designed to inventory and track IT hardware/software, personnel, and applications in place at agencies.
Information system	is a system of hardware, software and support that processes information electronically.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Information Technology	is all computerized and auxiliary automated information processing, telecommunication and related technology, including hardware, software, vendor support and related services, equipment and projects (ARS 41-3501(6)).
Information Technology Authorization Committee (ITAC)	is an executive, legislative, judicial, and private sector committee, which has planning, and oversight responsibility for information technology projects over $1 million in all three branches of State government. Legislation forming ITAC was enacted in 1996 and implemented July 1, 1997.
Information technology systems	are collectively the equipment used to create, store and transmit digital data and any related software owned (or otherwise controlled) and used by the State and its agencies to fulfill its service and obligations to the citizens of Arizona.
Informix®	is a relational database management system (RDBMS) that supports a wide variety of application development tools, along with a large number of other third-party tools, through support for the ODBC and JDBC industry standards for client connectivity. Informix is currently being merged with DB2®, and over time will be replaced by DB2®.
Ingres	is a relational database management system (RDBMS) that evolved from a research project at the University of California at Berkeley in the 1970s. There are two different versions of Ingres: a public domain version, known as University Ingres or Berkeley Ingres; and a commercial version currently marketed and known as OpenIngres. CA-OpenIngres™, or Ingres II™ runs on a variety of platforms and operating systems. Ingres has begun to add object-oriented development features to address the growing paradigm shift in the RDBMS marketplace towards more object-oriented database management systems (OODBMS). OpenIngres™ uses SQL and some forms of QUEL as its language for queries and database transactions. QUEL is a language developed for use with the original public domain version and still supported by it today.
Input/Output (I/O) devices	devices transfer data to/from a computer system involving communications channels, operator interface devices, and/or data acquisition and control interfaces.
Instant messaging	is real-time online e-mail. Instant messenger attachments typically bypass firewalls or gateways that scan for malicious content; if the content is encrypted either through the use of secure socket layer (SSL) or VPN services, detection is more difficult.
Instant Messaging and Presence Protocol (IMPP)	(RFC 2779) is an IETF Internet Working Group architecture for instant messaging and presence awareness/notification. It will specify how authentication, message integrity, encryption, and access control are integrated.
Institute of Electrical and Electronics Engineers, Inc (IEEE)	is a professional organization whose activities include the development of communications and network standards. IEEE LAN standards are the predominant LAN standards.
Integrated Services Digital Network (ISDN)	is a set of communications standards allowing a single wire or optical fiber to carry voice, digital network services, and video.
Integrity	in the context of information security, means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The loss of integrity is the unauthorized modification or destruction of information. [44 U.S.C., Sec. 3542]

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Intellectual property	is an idea, invention, process, program, or application that derives from the work of the mind or intellect – specifically, one that has had its ownership registered for the purpose of protection from unauthorized use by others (from Merriam-Webster's Dictionary of Law ©1996).
Intelligent Input/Output (I2O)	technology is a critical element of intelligent, high-performance, distributed I/O for Intel-based platforms, including the IA-64 processors. I2O provides a standards-based approach that complements existing drivers and offers a portable framework for the rapid development of a new generation of portable I/O solutions. I2O is the driver architecture of choice for intelligent storage and network devices with an input/output processor.
Interactive Connectivity Establishment (ICE)	is a methodology for Network Address Translator (NAT) traversal for the Session Initiation Protocol (SIP). ICE is not a new protocol, but rather makes use of existing protocols, such as Simple Traversal of UDP Through NAT (STUN), Traversal Using Relay NAT (TURN), and even Realm Specific IP (RSIP). ICE works through the cooperation of both endpoints in a session. This specification defines a general methodology that allows the media streams of multimedia signaling protocols to successfully traverse NAT. This methodology is independent of any particular signaling protocol.
Interagency Service Agreement (ISA)	is an agreement between agencies for specific services to be provided or exchanged.
Interface Definition Language (IDL)	is a generic term for a language that lets a program or object written in one language communicate with another program written in an unknown language. In distributed object technology, it is important that new objects are able to sent to any platform environment and discover how to execute in that environment. An Object Request Broker (ORB) is an example of a program that would use an interface definition language to "broker" communication between one object program and another one. Interface Definition Languages are the most visible components of a class of software known as "middleware," that class of software, which is neither part of an operating system nor an application, but is used to link together the various parts of a distributed application spread across geographically separated computers.
Interior Gateway Protocol (IGP)	is a protocol for exchanging routing information between gateways (hosts with routers) within an autonomous network (for example, a system of corporate local area networks). The routing information can then be used by the Internet Protocol (IP) or other network protocols to specify how to route transmissions.
InterNational Committee for Information Technology Standards (INCITS)	is the primary U.S. focus of standardization in the field of Information and Communications Technologies, encompassing storage, processing, transfer, display, management, organization, and retrieval of information. As such, INCITS also serves as ANSI's Technical Advisory Group for ISO/IEC Joint Technical Committee 1. JTC 1 is responsible for International standardization in the field of Information Technology.
International Electro-technical Commission (IEC)	is an industry group that writes and distributes standards for electrical products and components.
International Standards Organization (ISO)	is an international organization that is responsible for a wide range of standards, including those relevant to networking. ISO developed the OSI Reference Model.

Keyword	Description
International Telecommunication Union Telecommunication (ITU-T) Standardization Sector	is an international body that develops worldwide standards for telecommunications technologies. The ITU-T carries out the functions of the former CCITT.
Internet	is a wide area network connecting disparate networks worldwide. The Internet is also an international network of millions of web sites that uses TCP/IP protocol.
Internet Assigned Numbers Authority (IANA)	is an Internet central registry for the assigned values of the addresses (in the form of numbers) used in TCP/IP network protocol implementations.
Internet calendaring and scheduling (iCalendar)	as defined by IETF RFC 2445 provides the definition of a common format for openly exchanging calendaring and scheduling information across the Internet. IETF RFC 2445 is formatted as a registration for a MIME media type per IETF RFC 2048. The proposed media type value is 'text/calendar.' This MIME media type provides a standard content type for capturing calendar event, to-do, and journal entry information. It also can be used to convey free/busy time information. The content type is suitable as a MIME message entity that can be transferred over MIME-based email systems, using HTTP or some other Internet transport. In addition, the content type is useful as an object for interactions between desktop applications using the operating system clipboard, drag/drop, or file systems capabilities. ICalendar uses an Internet protocol called iCalendar Transport-Independent Interoperability Protocol (iTIP), defined in IETF RFC 2446, to specify how calendaring systems use iCalendar objects to interoperate with other calendar systems. RFC 2447 specifies a binding from iTIP to Internet email-based transports to convey iTIP over MIME as defined in IETF RFC 822 and 2045.
Internet Control Message Protocol (ICMP)	is a network layer Internet protocol that reports errors and provides other information relevant to IP packet processing.
Internet Engineering Task Force (IETF)	is a large, open, international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. IETF is generally recognized as the standards organization for the Internet.
Internet Group Management Protocol (IGMP)	is used by IP hosts to report their multicast group memberships to an adjacent multicast router.
Internet Inter-ORB Protocol (IIOP)	is a protocol that makes it possible for distributed applications written in different programming languages to communicate over the Internet. IIOP is a critical part of the industry CORBA standard. Using CORBA's IIOP and related protocols, applications can be written that will be able to communicate with existing or future applications wherever they are located and without having to understand anything about the application other than its service and a name. CORBA and IIOP are competing with a similar strategy from Microsoft® called the Distributed Component Object Model (DCOM). Microsoft® and the Object Management Group, sponsors of CORBA, have agreed to develop software bridges between the two models so that applications designed for CORBA can communicate with applications designed for DCOM.
Internet Message Access Protocol 4 (IMAP4)	is a standard protocol for accessing email from a local server. IMAP is a client/server protocol in which email is received and held for a user by an Internet server.

Keyword	Description
Internet Print Protocol (IPP)	is a client-server type protocol that should allow the server side to be either a separate print server or a printer with embedded networking capabilities. There is currently no universal standard for printing. Several protocols are in use, but each has limited applicability and none can be considered the prevalent one. IPP will include mechanisms to ensure adequate security protection for materials to be printed, including, at a minimum, mechanisms for mutual authentication of client and server, and mechanisms to protect the confidentiality of communications between client and server. This IETF Working Group has published several RFCs and Internet draft documents.
Internet Protocol (IP)	is the network layer protocol in the TCP/IP stack offering a connectionless internetwork service. IP provides features for addressing, type-of-service specification, fragmentation and reassembly, and security. IPv4 routes each packet based on a 32-bit destination address called an IP address (e.g., 123.122.211.111). IPv6 uses a sixteen-octet 128-bit IP address.
Internet Protocol Security Protocol (IPSec)	is a suite of protocols that handles encryption, authentication, and secure transport of IP packets. It currently consists of numerous Internet Drafts and RFCs produced by the IETF IPsec working group. IPSec will provide network-layer security for IPv4 and IPv6. IPSec works at Layer 3 to transport data transparently to network applications. It is intended to provide more lower-level security than SSL (Secure Socket Layer). IPSec adds a header to packets being sent over a VPN to identify that those packets that have been secured. It supports several types of encryption including the Data Encryption Standard (DES) and Message Digest 5 (MD5), and two kinds of key management schemes that allow parties to agree upon parameters for the session. Proposals call for adding additional security features. IPSec also provides for data compression, which partially compensates for the poor compression that modems are able to perform on encrypted data. IPSec does not provide support for network address translation.
Internet Service Provider (ISP)	is a company that provides Internet access to other companies and individuals.
Internet user	is an agency employee, contract employee or other agency-authorized person who accesses the Internet through the use of state/agency owned and/or controlled information technology.
Internet Voice Messaging (IVM)	provides for the carriage of voicemail messages over Internet mail as part of a unified messaging infrastructure. The Internet Voice Messaging (IVM) IETF draft concept is not a successor format to VPIM v2, but rather an alternative specification for a different application.
Internetwork Packet Exchange (IPX)	is the Novell NetWare network layer (Layer 3) protocol used for transferring data from servers to workstations. IPX is similar to IP.
Internetworking devices	include routers, firewalls, and switches. These items provide access to and information about networks and, therefore, must be strictly controlled to prevent unauthorized access.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Interoperability	is 1. The ability of Information Technology (IT) systems to provide services to and accept services from other IT systems and to use the services so exchanged to enable them to operate effectively together. 2. The ability of disparate systems to be linked together and then operate as a single entity through the exchange of information facilitated through open standards or non-proprietary protocols.
Intranet	is a limited collection of interconnected LANs and standalone computers. An Intranet functions the same as the Internet, using the same user interfaces and file transfer protocols. The difference between an Internet and an Intranet is that an Intranet provides connectivity only between specific sites in order to create a pre-determined infrastructure for business units, customers, or designated participants.
Intrusion Detection Systems (IDS)	detect break-ins or break-in attempts manually or via software expert systems that operate on logs or other information available on the network. Pertaining to techniques that attempt to detect intrusion into a computer or network by observation of security logs or audit data.
Investment	is the sum of vendor, construction, energy, facilities and telecommunication costs.
IP Quality of Service Protocols: 802.1p Priority and VLAN Topology	is a Layer 2 method for signaling network priority on a per-frame basis. It consists of 1. a prioritization component allows network managers to assign priorities to specific packets. It provides for 8 different priorities for Level-2 traffic based on a 3-bit "User Priority" field defined by 802.1Q, and 2. GARP (Group Address Registration Protocol) lets switches and end-stations exchange VLAN topology information. In addition to defining priority, 802.1p introduces a new protocol: the Generic Attributes Registration Protocol (GARP). Two specific implementations of this protocol have been defined. The first of these is the GARP Multicast Registration Protocol (GMRP), which lets workstations request membership in a multicast domain. The second protocol is the GARP VLAN Registration Protocol (GVRP). GVRP is similar to GMRP, but instead of requesting admission to a multicast domain, the workstation requests admission to a particular VLAN. This protocol links 802.1p and 802.1Q. 802.1Q VLAN Tagging defines changes to Ethernet frames that will enable them to carry VLAN information. It allows switches to assign end-stations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks. Four bytes have been added to the Ethernet frame for this purpose, causing the maximum Ethernet frame length to increase from 1518 to 1522 bytes. In these 4 bytes, 3 bits allow for up to eight priority levels and 12 bits identify one of 4,094 different VLANs. 802.3ac will define the specifics of these changes for Ethernet frames. 802.1p specifies a method for indicating frame priority based on the new fields. The missions of 802.1p and 802.1Q are to provide a uniform method for conveying frame priority and VLAN trunking information across the network.
IP telephony	is a general term for the technologies that use the IP packet-switched connections to exchange voice, fax, and other forms of information that have traditionally been carried over the dedicated circuit-switched connections of the public switched telephone network (PSTN). The IETF Working Group currently has published several RFCs and Internet draft documents. IP telephony is the result of the transformation of the circuit-switched telephone network to a packet-based network that deploys voice-compression algorithms and flexible and sophisticated transmission techniques. It delivers richer services using only a fraction of traditional digital telephony's usual bandwidth.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
ISO/IEC 11179	is a set of six standards that promote the sharing and reusability of data by providing guidelines for attribute specification standardization. It provides the standardized descriptions and structure of like data, improving portability and reuse, while reducing duplication of data. Part 1: Framework for the specification and standardization of data, Part 2: Classification for data elements, Part 3: Basic attributes of data elements and associated metadata, and registry metamodel, Part 4: Rules and guidelines for the formulation of data definitions, Part 5: Naming and identification principles for data elements, and Part 6: Registration of data elements.
J2ME (Java 2 Platform, Micro Edition)	is a technology that allows programmers to use the Java programming language and related tools to develop programs for mobile wireless information devices such as cellular phones and personal digital assistants (PDAs). J2ME consists of programming specifications and a special virtual machine, the K Virtual Machine, which allows a J2ME-encoded program to run in the mobile device. There are two programming specifications: Connected, Limited Device Configuration (CLDC) and the Mobile Information Device Profile (MIDP). CLDC lays out the application program interface (API) and virtual machine features needed to support mobile devices. MIDP adds to the CLDC the user interface, networking, and messaging details needed to interface with mobile devices. MIDP includes the idea of a midlet, a small Java application similar to an applet but one that conforms to CLDC and MIDP and is intended for mobile devices
Java 2 Platform Edition (J2EE) Connector Architecture Specification	defines a standard architecture for connecting the J2EE platform to heterogeneous enterprise information systems.
Java 2 Platform, Enterprise Edition™ (J2EE)	is a Java™ platform designed for mainframe-scale computing. J2EE™ is designed to simplify application development in a thin-client tiered environment. J2EE™ simplifies application development and decreases the need for programming and programmer training by creating standardized, reusable, modular components and by enabling the tier to handle many aspects of programming automatically.
Java API for XML Processing (JAXP)	supports processing of XML documents using DOM, SAX, and XSLT. JAXP enables applications to parse and transform XML documents independent of a particular XML processing implementation.
Java API for XML Registries (JAXR)	provides a uniform and standard Java API for accessing different kinds of XML Registries. An XML registry is an enabling infrastructure for building, deploying, and discovering Web services. JAX-RPC (Java API for XML-Based RPC) is an application program interface (API) in the Java Web Services Developer Pack (WSDP) that enables Java developers to include remote procedure calls (RPCs) with web services or other Web-based applications. JAX-RPC is aimed at making it easier for applications or Web services to call other applications or Web services. JAX-RPC provides a programming model for the development of SOAP (Simple Object Access Protocol)-based applications. The JAX-RPC programming model simplifies development by abstracting SOAP protocol-level runtime mechanisms and providing mapping services between Java and the Web Services Description Language (WSDL).

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Java Architecture for XML Binding (JAXB)	provides an API and tools that automate the mapping between XML documents and Java objects. JAXB makes XML easy to use by compiling an XML schema into one or more Java technology classes. The combination of the schema derived classes and the binding framework enable one to perform the following operations on an XML document.
Java Data Objects (JDO)	is an application program interface (API) that enables a Java programmer to access a database implicitly - that is, without having to make explicit Structured Query Language (SQL) statements. JDO is recommended as a complement to Java Database Connectivity (JDBC), the interface that supports access to popular database programs using SQL statements. Using JDO, the programmer uses classes to define data objects and the supporting program manages the actual access of data from a given database based on the class definitions.
Java Database Connectivity (JDBC) Data Access API	provides cross-DBMS connectivity to a wide range of SQL databases and also provides access to other tabular data sources, such as spreadsheets or flat files.
Java Database Connectivity™ (JDBC)	is an Application Program Interface (API) specification for connecting programs written in Java™ to the data in databases. The API allows encoding access request statements in SQL that are then passed to the program that manages the database. It returns the results through a similar interface. JDBC™ is very similar to the SQL Access Group's Open Database Connectivity (ODBC) and, with a "bridge" program, the JDBC™ interface can be used to access databases through the ODBC interface.
Java Message Service™ (JMS)	is an Application Program Interface (API) that supports the formal communication known as “messaging” between devices in a network. JMS™ provides a common interface to standard messaging protocols and to special messaging services in support of Java™ programs.
Java Server Page (JSP)	is a technology for controlling the content or appearance of Web pages using servlets, small programs that are specified in the Web page and run on the Web server to modify the Web page before it is sent to the user who requested it. Sun Microsystems, the developer of Java, also refers to the JSP technology as the Servlet application program interface (API).
Java Servlet technology	provides a component-based, platform-independent method for building Web-based applications.
Java Transaction API (JTA)	is a high level, implementation independent, protocol independent API that allows applications and application servers to access transactions.
Java Transaction Service (JTS)	specifies the implementation of a Transaction Manager which supports Java Transaction API (JTA) and implements the Java mapping of the Object Management Group (OMG) Object Transaction Service specification. JTS propagates transactions using the Internet Inter-ORB Protocol (IIOP).
Java Virtual Machine (VM)	is the component of the Java technology that is responsible for its hardware and operating system independence. It is designed to support multiple host architectures and to allow secure delivery of software components. The Java VM does not assume any particular implementation technology, host hardware, or host operating system. It is not inherently interpreted, but can just as well be implemented by compiling its instruction set to that of a silicon CPU. Java VM may also be implemented in micro code or directly in silicon.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Java™	is a programming language expressly designed for portability and use in the distributed environment of the Internet. It was designed to have the "look and feel" of the C++ language, but it is simpler to use than C++ and enforces an object-oriented programming model. Java™ can be used to create complete applications that may execute on a single computer or distributed among servers and clients in a network. It can also be used to build a small application module or applet for use as part of a Web page. Applets make it possible for a Web page user to interact with the page.
Java™ Naming and Directory Interface (JNDI)	is an industry-wide, open interface that gives developers a common interface for navigating the many naming systems that exist in the computing world today. JNDI greatly simplifies the code needed to browse directory services such as eDirectory, X.500, and LDAP. JNDI enables Java platform-based applications to access multiple naming and directory services. Part of the Java Enterprise application programming interface (API) set, JNDI makes it possible for developers to create portable applications that are enabled for Lightweight Directory Access Protocol (LDAP) and distributed object systems such as the Common Object Request Broker Architecture (CORBA), Java Remote Method Invocation (RMI), and Enterprise JavaBeans (EJB)
Jini	is referred to as "spontaneous networking." Using the Jini architecture, users will be able to plug printers, storage devices, speakers, and any kind of device directly into a network and every other computer, device, and user on the network will know that the new device has been added and is available. Each pluggable device will define itself immediately to a network device registry. When someone wants to use or access the resource, their computer will be able to download the necessary programming from it to communicate with it. The operating system will know about all accessible devices through the network registry. Jini can be viewed as the next step after the Java programming language toward making a network look like one large computer.
Jini technology	is referred to as "spontaneous networking." The Jini architecture will allow users to plug printers, storage devices, or any kind of device directly into a network and enable every other computer, device, and user on the network to know that the new device has been added and is available. Each pluggable device will define itself immediately to a network device registry. The operating system will know about all accessible devices through the network registry. Jini can be viewed as the next step after the Java programming language toward making a network look like one large computer.
Joint Photographic Experts Group (JPEG)	is a widely used industry-standard graphic image file format (ISO Standard 10918). JPEG is an acronym for Joint Photographic Experts Group, the committee that established the baseline algorithms.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Kerberos	is a secret-key network authentication protocol implemented through Authentication, Authorization, and Accounting (AAA) that uses the Data Encryption Standard (DES) cryptographic algorithm for encryption and authentication. Kerberos was designed to authenticate requests for network resources. Kerberos is based on the concept of a trusted third party that performs secure verification of users and services. The primary use of Kerberos is to verify that users and the network services they use are really who and what they claim to be. To accomplish this, a trusted Kerberos server issues tickets to users. These tickets, which have a limited lifespan, are stored in a user's credential cache and can be used in place of the standard username-and-password authentication mechanism.
Key pair	refers to a private key and its corresponding public key in an asymmetric crypto-system. The key pair is unique in that the public key can verify a digital signature that the private key creates or a private key can un-encrypt a message or file that a public key encrypts
Key system	or Key Telephone System is a system in which the telephones have multiple buttons permitting the user to select central office phone lines or intercom lines.
Laptop	is a small, notebook-sized computer containing the functionality of a desktop computer. A laptop may be turned into a desktop computer with a docking station, a hardware frame that supplies connections for peripheral input/output devices such as a printer or larger monitor.
Layer 2 Forwarding Protocol (L2F)	is the underlying link-level technology for both multi-chassis multi-link PPP Protocol (MP - see IETF RFC 1717) and Virtual Private Networks (VPN). The virtual dial-in services functionality is based on the L2F protocol IETF draft RFC. The L2F protocol focuses on providing a standards- based tunneling mechanism for transporting link-layer frames (for example, High-Level Data Link Control (HDLC), asynchronous Point-to-Point Protocol (PPP - see IETF RFC 1331) of higher-layer protocols. Using such tunnels, it is possible to divorce the location of the initial dial-in server from the location at which the dial-in protocol connection is terminated and the location at which access to the network is provided.
Least privilege	is a security administration principle specifying that only the minimum level of access authorization be provided to complete the assigned task or role.
Lightweight Directory Access Protocol (LDAP)	is a protocol that enables access for management and browser applications that provide read/write interactive access to the X.500 Directory, which is a standard for directory services in a network.
Link Control Protocol (LCP)	is the protocol that establishes, configures, and tests data-link connections for use by Point-to-Point Protocol (PPP).
Local Area Network (LAN)	is a communications system of multiple interconnected workstations, peripherals, data terminals, or other devices confined to a limited geographic area consisting of a single building or a cluster of buildings.
Local Exchange Carriers (LECs)	are local telephone companies: e.g., Qwest Communications and Citizens Communications. Often, these include competitive local exchange carriers (CLECs).

Keyword	Description
Logical Link Control (LLC)	is the higher of the two data link layer sub-layers defined by the IEEE. The LLC sub-layer handles error control, flow control, framing, and MAC-sub-layer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants.
Machine code	is the elemental language of computers, consisting of a stream of 0's and 1's. Ultimately, the output of any programming language analysis and processing is machine code.
Macro viruses	represent the second generation of virus threat and spreads by means of macroinstructions that are found in office applications such as Microsoft® Word® (word processor) and Microsoft® Excel® (spreadsheet). The macros are typically stored as part of a document and can be transported as attachments to e-mail messages. Any application that supports automatically executable macros is a potential carrier for macro viruses, and because of the increasing use of the Internet, macro viruses are becoming more and more problematic. When a file containing an infected macro is used, the infected file reproduces into an application from which it will infect other Word® or Excel® files. These type of viruses are not detected by traditional scanning engines, but can be detected using a heuristics approach.
Mainframe	is an industry term for a large computer, typically manufactured for commercial applications of Fortune 1000 businesses and other large-scale computing purposes. Historically, a mainframe is associated with centralized rather than distributed computing. Today, manufacturers refer to their larger processors as large servers and emphasizes that they can be used to serve distributed users and smaller servers in a computing network.
Malware	(for "malicious software") is programming or files that are developed for the purpose of doing harm. Thus, malware includes computer virues, worms, and Trojan Horses.
Management Information Base (MIB)	is a database of network management information that is used and maintained by a network management protocol, such as SNMP. An MIB object can be changed or retrieved through a GUI network management system using SNMP commands. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.
May	identifies acceptable activities.
Mean opinion score (MOS)	provides a numerical measure of the quality of human speech at the destination end of a connection. The scheme uses subjective tests (opinionated scores) that are mathematically averaged to obtain a quantitative indicator of the system performance. The MOS is the arithmetic mean of all the individual scores, and can range from 1 (worst) to 5 (best).
Media Access Control (MAC)	is the IEEE 802 protocol defining media-specific access control. It is the lower of the two sub-layers of the data link layer. The MAC sub-layer handles access to shared media, such as whether token passing or contention will be used.
Mesh networks	are those having many nodes, which are connected by multiple links.
Message	is the application layer (Layer 7) logical grouping of information, often composed of a number of lower-layer logical groupings, such as packets.

Keyword	Description
Message Digests	are used to ensure the integrity of information. Integrity means that information cannot be altered without detection. Information is put through a mathematical function that creates a 'hash' or message digest. Even the slightest change to the information would generate a different message digest if the mathematical function were performed again. To verify information has not been modified, a user applies the same hash function on the selected information to generate another message digest. If the resulting message digest matches the original message digest, the information has not been changed.
Messaging Application Program Interface (MAPI)	is a Microsoft® Windows™ program interface that enables a user to send email from within a Windows™ application and attach the document to the e-mail message. Applications that take advantage of MAPI include word processors, spreadsheets, and graphics applications. MAPI-compatible applications typically include a "Send Mail" or "Send" feature in the "File" pull-down menu.
Messaging-Oriented Middleware (MOM)	, provides applications with the ability to send and receive messages across platforms. The messages contain application-specified information and/or directives meaningful within the context of the application. The message is queued and made available to one or more target applications. Presently, there are no standards for MOM; therefore, only those software applications that use the same MOM products can interoperate.
Meta Data Interchange Specification (MDIS)	is a non-proprietary and extensible mechanism from the Meta Data Coalition for the interchange of metadata between MDIS-aware tools.
Meta directory services	allow organizations to continue to use special purpose directories (i.e. network operating systems and application directories) and to build a directory infrastructure that takes advantage of the special information in those directories for enterprise-wide use.
Metadata	is information about data, including the format of the data element, which application system owns it, where it is located, and how it should be used. Metadata is the global information about what data exists across the enterprise and the standards applying to that data. It is very important to the data warehouse effort because it sets the standards and the rules used for data transformation and cleansing.
Meta-Object Facility (MOF™)	is an extensible model driven integration framework for defining, interchanging, manipulating, and integrating metadata and data in a platform independent manner. MOF-based standards are in use for integrating tools, applications, and data. MOF™ bridges the gap between dissimilar meta-models by providing a common basis for meta-models. If two different meta-models are both MOF-conformant, then models based on them can reside in the same repository. MOF is an OMG metadata interface specification that can be used to define and manipulate a set of interoperable metamodels and their instances. MOF also defines a UML-based meta-metamodel to describe metamodels in various domains.
Metropolitan Area Network (MAN)	is a communications system that spans a metropolitan area. MANs cover more geographic area than LANs, but less than wide-area networks (WANs).

Keyword	Description
Microsoft® Office	is a productivity software suite of products that includes: Microsoft® Word® (word processor), Microsoft® Excel® (spreadsheet), Microsoft® Access® (relational database), Microsoft® PowerPoint® (presentation graphics) and Microsoft® Outlook® (personal information manager and communication solution, email client)
Microwave	is a data transmission method using a series of towers that have been erected along a line of sight over the terrain of a wide area, usually in conjunction with the Public Switched Telephone Network (PSTN).
Middlebox Communications (Midcom)	(RFC 3303, 3304) is an emerging IETF protocol that addresses the issue of encrypted communications, making firewalls and NATs controllable through third parties. MidCom has the task of opening and closing transport ports (UDP and TCP) and managing NAT mappings at the firewall or NAT. A MidCom protocol agent, residing on the firewall, dynamically opens pinholes upon request of the SIP proxy or standard gatekeeper. By doing this, the firewalls or NATs continue to support secure services while remaining protocol agnostic at the application level.
Middleware	is software that facilitates and simplifies communication within and between services, application systems, and components, whether distributed or not, or running on heterogeneous platforms (or not). Middleware facilitates interchange of information in a distributed, multi-vendor, and heterogeneous systems environment while providing the same levels of security, reliability, and manageability traditionally associated with a monolithic, mainframe-based architecture where all products are supplied by a single vendor. More specifically, the term refers to an evolving layer of services that resides between the network and more traditional applications for managing security, access, and information exchange.
Mobile agents	are autonomous software entities that can halt their execution, transport themselves to another agent-enabled host on the network, and continue their execution on the new host, deciding where to go and what to do along the way. Mobile agents are goal-oriented, adaptive, can communicate with other agents, and can continue to operate even after the machine that launched them has been removed from the network.
Mobile IP	is an Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining their permanent IP address. Defined in RFC 3344 for IPv4, which obsoletes RFC 2002, Mobile IP is an enhancement of the Internet Protocol (IP) that adds mechanisms for forwarding Internet traffic to mobile devices (known as mobile nodess) when they are connecting through other than their home network.
Modems	are communication devices that modulate outgoing digital signals from a computer or other digital device to analog signals for a conventional telephone line, demodulate the incoming analog signal, and convert it to a digital signal for the digital device.
Monolithic applications	, refer to Application Architecture Perspectives.
Motherboard	is the physical arrangement in a computer that contains the computer's basic circuitry and components.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Moving Picture Experts Group (MPEG)	, in conjunction with ISO, develops standards for digital video and digital audio compression. The MPEG standards are an evolving series, each designed for a different purpose. MPEG-1 was designed for coding progressive video at a transmission rate of about 1.5 million bits per second. MPEG-2 was designed for coding interlaced images at transmission rates above 4 million bits per second. A proposed MPEG-3 standard, intended for High Definition TV (HDTV), was merged with the MPEG-2 standard when it became apparent that the MPEG-2 standard met the HDTV requirements. MPEG-4 is a standard that addresses speech and video synthesis, fractal geometry, computer visualization, and an artificial intelligence approach to reconstructing images. MPEG-4 addresses a standard way for authors to create and define the media objects in a multimedia presentation. It defines how objects can be synchronized and related to each other in transmission, and how users are to be able to interact with the media objects. MPEG-21, in draft stage, provides a larger, architectural framework for the creation and delivery of multimedia.
Multicast	is a method to distribute information where single packets are copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address Field.
Multidimensional databases (MDBs)	are a type of database that is optimized for data warehouse and online analytical processing (OLAP) applications. Multidimensional databases are frequently created using input from existing relational databases. Whereas a relational database is typically accessed using a Structured Query Language (SQL) query, a multidimensional database allows a user to ask questions related to summarizing business operations and trends. An OLAP application that accesses data from a multidimensional database is known as a MOLAP (multidimensional OLAP) application
Multifactor Authentication	is also referred to as strong authentication in which individual authentication methods are combined together. A common type is two-factor authentication, such as using a PIN code as well as a secure token to log on to a network.
Multi-Mode Optical Fiber (MMF)	has many propagation paths for light, typically used for lower speeds or shorter distances (as compared to single-mode optical fiber).
Multiplexing	is sending multiple signals or streams of information on a carrier at the same time in the form of a single, complex signal and then recovering the separate signals at the receiving end.
Multiprotocol Border Gateway Protocol (MBGP)	, based on RFC 2283, is an extension to BGP that provides scalable policy-based inter-domain routing
Multiprotocol Label Switching (MPLS)	fuses the intelligence of routing with the performance of switching and provides significant benefits to networks with a pure IP architecture as well as those with IP and ATM or a mix of other Layer 2 technologies. MPLS technology is instrumental to scalable virtual private networks (VPNs) and end-to-end quality of service (QoS), enabling efficient utilization of existing networks to meet future growth and rapid fault correction of link and node failure. The technology also helps deliver highly scalable, differentiated end-to-end IP services with simpler configuration, management, and provisioning for both Internet providers and subscribers.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Multi-Purpose Internet Mail Extensions (MIME)	is an extension of the original Internet email protocol that expands use of the protocol to exchange different kinds of data files on the Internet: audio, video, images, application programs, and other kinds, as well as the ASCII text handled in the original protocol, Simple Mail Transport Protocol (SMTP). New MIME data types are registered with the Internet Assigned Numbers Authority (IANA). MIME is specified in detail in IETF RFC 1521 and 1522, which amend the original mail protocol specification, IETF RFC 821 (the Simple Mail Transport Protocol) and the ASCII messaging header, IETF RFC 822.
National Association of State Chief Information Officers (NASCIO)	The mission of the association is to shape national IT policy through collaborative partnerships, information sharing and knowledge transfer across jurisdictional and functional boundaries.
National Committee for Information Technology Standards (NCITS)	is an ANSI accredited Standards Development Organization charged with the development of timely and relevant information technology standards.
National Institute of Standards and Technology (NIST)	is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurements, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.
Natural	is a 4GL programming language. It was designed specifically for building mission-critical applications. The three-tier architecture (front-end, business logic, data storage) of this component-based environment guarantees outstanding flexibility. Natural-built applications are ideal for cross-platform, cross-enterprise, and even inter-enterprise environments. Natural applications support all leading platforms and can be integrated seamlessly with all the major database systems (Adabas™, DB2®, Oracle®, etc.). Natural is available on many platforms from mainframe servers to client devices. Natural source code can be moved easily between these platforms, allowing its user to switch between server technologies when traffic rates change. Natural can be integrated with components written in other languages, such as C, Java™, Visual Basic®, or COBOL.
NET	is a collection of programming support for what are known as Web services, the ability to use the Web rather than a PC for various services. Microsoft's goal is to provide individual and business users with a seamlessly interoperable and Web-enabled interface for applications and computing devices and to make computing activities increasingly Web-browser-oriented. The .NET platform includes servers; building block services, such as Web-based data storage; and device software. The .NET platform is expected to provide the ability to make the entire range of computing devices work together and to have user information automatically updated and synchronized on all of them, increased interactive capability for Web sites, enabled by greater use of XML rather than HTML, generalized data storage that will increase efficiency and ease of access to information, as well as synchronization of information among users and devices, and the ability to integrate various communications media, such as e-mail, faxes, and telephones.
NetBIOS Extended User Interface (NetBEUI)	is the enhanced version of the NetBIOS protocol used by network operating systems such as LAN Manager, LAN Server, and Windows for Workgroups™, and Windows NT™. NetBEUI formalizes the transport frame and adds additional functions. NetBEUI implements the OSI LLC2 protocol.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Network	is a configuration of devices and software connected for information interchange. A network is commonly considered a collection of two or more computer systems linked together. A Converged Network uses Internet Protocol (IP) to send data, voice, and video across a single network channel, which enables greater collaboration, simplifies network management, and reduces operating costs.
Network Address Translation (NAT)	is a mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.
Network Attached Storage (NAS)	is a file-oriented storage implementation where storage devices are connected to a network and provide file access services to computer systems. A NAS storage element consists of an engine, which implements the file services, and one or more devices, on which data is stored. NAS elements may be attached to any type of network. When attached to SANs, NAS elements may be considered to be members of the SAS class of storage elements. A host system that uses network-attached storage uses a file system device driver to access data using file access protocols such as NFS or CIFS. NAS systems interpret these commands and perform the internal file and device I/O operations necessary to execute them.
Network Basic Input/Output System (NetBIOS)	is an API used by applications on an IBM LAN to request services from lower-level network processes. These services might include session establishment and termination, as well as information transfer.
Network Control Protocol (NCP)	is a series of protocols for establishing and configuring different network layer protocols, such as Point-to-Point Protocol (PPP).
Network Data Management Protocol (NDMP)	is an open standards protocol defined by the Network Data Management Task Force. NDMP allows a backup application to control the retrieval of data from a storage subsystem or NAS device and copy it directly to a second storage device (normally a tape drive) across the network. NDMP is a communications protocol that allows intelligent devices on which data is stored, robotic library devices, and backup applications to intercommunicate for performing backups. NDMP allows a network backup application to control the retrieval of data from, and backup of, a server without third-party software. The control and data transfer components of backup and restore are separated. NDMP is intended to support tape drives, but can be extended to address other devices and media in the future.
Network File System (NFS)	has become a de facto standard protocol (version 4 is defined by IETF RFC 3010). Particularly common on UNIX-based systems, NFS implementations are available for virtually every modern computing platform in current use, from desktops to supercomputers.
Network Interface Card (NIC)	is a board that provides network communication capabilities to and from a computer system.
Network Service Access Point (NSAP)	is a network address, as specified by ISO. An NSAP is the point at which OSI network service is made available to a transport layer (Layer 4) entity.

Keyword	Description
Non-repudiation	security service provides protection against false denial of involvement in a communication. 1. Non-repudiation with proof of origin provides the recipient of data be provided with proof of origin of the data. This protects against any subsequent attempt by the sender to falsely deny sending the data or its contents. 2. Non-repudiation with proof of delivery provides the sender of data be provided with proof of delivery of data. This protects against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.
n-tier oriented application architecture	, refer to Application Architecture Perspectives.
Object identifier (OID)	Values are defined in specific MIB modules. The Event MIB allows a user or a network management system to watch over specified objects and to set event triggers based on existence, threshold, and Boolean tests. An event occurs when a trigger condition is justified; this means that a specified test on an object returns a value of true. The MIB can be configured so that when triggers are activated, an SNMP Set is performed, a notification is sent out to the interested host, or both.
Object Management Group (OMG)	was formed to create a standard architecture for distributed objects in networks. The architecture that resulted is the Common Object Request Broker Architecture (CORBA). A central element in CORBA is the Object Request Broker (ORB). An ORB makes it possible for a client object to make a server request without having to know where in a network the server object or component is located and exactly what its interfaces are. A number of middleware software products use CORBA and it appears to be a strategic architecture for distributed objects. The OMG now has over 500 member companies.
Object Request Broker (ORB)	provides the means for communicating between application objects (components) residing on different platforms. ORB is an essential concept in CORBA. ORB support in a network of clients and servers on different computers means that a client application (which may itself be an object) can request services from a server application or object without having to understand where the server is in a distributed network or what the interface to the server application looks like. To make requests or return replies between the ORBs, applications use the General Inter-ORB Protocol (GIOP) and Internet Inter-ORB Protocol (IIOP). IIOP maps GIOP requests and replies to the Transmission Control Protocol (TCP) layer in each device.
Object-Oriented Database Management Systems (OODBMS)	are database management systems that support the modeling and creation of data as objects. There is currently no agreed-upon standard for what constitutes an OODBMS, and OODBMS products are considered to be still in their infancy. The Object Data Management Group (ODMG) is developing an object-oriented database interface standard.
Object-Oriented Programming (OOP)	is organized around "objects" rather than "actions," data rather than logic. Historically, a program has been viewed as a logical procedure that takes input data, processes it, and produces output data. The programming challenge was seen as how to write the logic, not how to define the data. Object-oriented programming takes the view that business functions care about the objects to manipulate, rather than the logic required to manipulate them. The first step in OOP is to identify all the objects and how they relate to each other, an exercise often referred as data modeling.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Object-Relational Database Management Systems (ORDBMS)	incorporate the concept that object-oriented database concepts can be superimposed on relational databases. The Object Management Group (OMG) has already standardized an object-oriented, data-brokering interface between systems in a network.
Objects	, in object-oriented programming (OOP), are the fundamental program design elements and are the resulting units of code that are produced from the programming process. Each object is incorporated into a generic class [template definition of the methods (programmed procedures) and variables (values that can change, depending on conditions or on information passed to the program) in a particular kind of object] of objects. Classes of objects are also defined so that objects can share models and reuse the class definitions in their code. Examples of objects range from human beings (described by name, address, etc.) to buildings and floors (whose properties can be described and managed) down to the components on a device.
Obsolescent	is one of four categories used in the PSP program and EA to guide technology use in the State of Arizona (see also emerging, strategic, and transitional). “Obsolescent” implies that the State’s Enterprise Architecture actively promotes that agencies employ a different technology. Agencies should not plan new deployments of this technology and instead should develop a plan to replace it. This technology may be waning in use or no longer supported.
OLE DB	is a low-level application program interface (API) for access to different data sources. OLE DB includes not only the Structured Query Language (SQL) capabilities of the standard data interface Open Database Connectivity (ODBC) but also includes access to data other than SQL data.
Omnis 7	is an integrated development environment for Windows™ and Macintosh end users.
Online Analytical Processing (OLAP)	is computer processing that enables a user to easily and selectively extract and view data from different points-of-view. OLAP data is stored in a multidimensional database. Whereas a relational database can be thought of as two-dimensional, a multidimensional database considers each data attribute as a separate "dimension." OLAP software can locate the intersection of dimensions and display them. OLAP can be used for data mining or the discovery of previously undiscerned relationships between data items. An OLAP database does not need to be as large as a data warehouse, since not all transactional data is needed for trend analysis. Using Open Database Connectivity (ODBC), data can be imported from existing relational databases to create a multidimensional database for OLAP.
Online Transaction Processing (OLTP)	is a class of program that facilitates and manages transaction-oriented applications, typically for data entry and retrieval transactions in a number of industries.

Keyword	Description
Open Architecture	is 1. The process, overall structure, framework, logical components, and logical interrelationships that are based on open-industry-standards and pervasive industry de facto standards, rather than on closed, proprietary design. Conceptually, an architecture that is open will facilitate interoperability, portability, and scalability as well as provide competitive choices and solutions. 2. the layered hierarchical structure, configuration, or model of a communications or distributed data processing system that (a) enables system description, design, development, installation, operation, improvement, and maintenance to be performed at a given layer or layers in the hierarchical structure, (b) allows each layer to provide a set of accessible functions that can be controlled and used by the functions in the layer above it, (c) enables each layer to be implemented without affecting the implementation of other layers, and (d) allows the alteration of system performance by the modification of one or more layers without altering the existing equipment, procedures, and protocols at the remaining layers. Note: Examples of independent alterations include (a) converting from wire to optical fibers at a physical layer without affecting the data-link layer or the network layer except to provide more traffic capacity, and (b) altering the operational protocols at the network level without altering the physical layer.
Open Database Connectivity (ODBC	is an open standard Application Program Interface (API) for accessing a database. ODBC is based on and closely aligned with The Open Group standard Structured Query Language (SQL) Call-Level Interface. It allows programs to use SQL requests that will access databases without having to know the proprietary interfaces to the databases. ODBC handles the SQL request and converts it into a request the individual database system understands.
Open Group	is a software standards organization that is sponsored by a number of major software vendors. The Open Group develops and fosters industry standards for software interfaces, often using technologies developed by one of the sponsoring companies. The Open Group originated by combining two previous organizations, X/Open and the Open Software Foundation (OSF). Standards that the Open Group maintains include the standard UNIX program interfaces and SQL.
Open Shortest Path First (OSPF)	is a routing protocol (IETF RFC2328) developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force (IETF) to determine the best path for routing IP traffic over a TCP/IP network. It was developed to create less route-calculation traffic between routers than the RIP protocol. OSPF v3 is the most recent version that accommodates IPv6.
Open Software Foundation (OSF)	was an industry-sponsored organization whose purpose was to foster, identify, and, in some cases, develop software technologies that could serve as industry and perhaps eventually national and international standards. OSF developed a widely implemented, cross-platform, industry-standard for distributed computing, the Distributed Computing Environment (DCE). OSF has been incorporated into The Open Group.
Open standard	is a standard that is not proprietary to a specific manufacturer, vendor, product, or owner, but may be used among various components and products such that it facilitates interoperability; and that has been approved by an appropriate national or international standards body.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Open system	is a system whose characteristics comply with standards made available throughout the industry and which therefore can be connected to other systems complying with the same standards.
Open System Interconnection (OSI) Layer 7 Reference Model	is a network architectural model developed by ISO and ITU-T. The model consists of seven layers, each of which specifies particular network functions, such as addressing, flow control, error control, encapsulation, and reliable message transfer. The lowest layer (the physical layer) is closest to the media technology. The lower two layers are implemented in both hardware and software, whereas the upper five layers are implemented only in software. The highest layer (the application layer) is closest to the user. The OSI reference model is used universally as a method for teaching and understanding network functionality.
Operating Systems (OS)	are 1. The programs that, after being initially loaded, manage all other programs (applications) in a device. The application programs make use of the operating system by making requests for services through a defined Application Program Interface (API). In addition, users can interact directly with the operating system through a user interface such as a command language or a Graphical User Interface (GUI). 2. An integrated collection of routines that service the sequencing and processing of programs by a computer. Note: An operating system may provide many services, such as resource allocation, scheduling, input/output control, and data management. Although, operating systems are predominantly software, partial or complete hardware implementations may be made in the form of firmware.
Oracle®	is a relational database management system (RDBMS) with associated application development tools that is available for a variety of platforms and operating systems. Oracle® fully utilizes XML and other e-Business Oracle's relational database was the world's first to support the Structured Query Language (SQL), now an industry standard.
Organization for the Advancement of Structured Information Standards (OASIS)	is a not-for-profit, global consortium that drives the development, convergence, and adoption of e-Business standards. Members themselves set the OASIS technical agenda, using a lightweight, open process expressly designed to promote industry consensus and unite disparate efforts. OASIS produces worldwide standards for security, Web services, XML conformance, business transactions, electronic publishing, topic maps, and interoperability within and between marketplaces.
Original Equipment Manufacturer (OEM)	of hardware and software products.
Out-of-band communication	refers to a communication device, platform, or media other than that communication media or platform on which a suspected or actual security threat is occurring. Thus, it becomes the alternative communication device, platform, or media used to report an incident.
Owner	refers to that group (i.e., Agency or Agency unit) which controls a set of information resources and determines its level of criticality and sensitivity. As such, they determine access, authorization rights, and dissemination regarding those resources.
PACE COBOL®	, along with the PACE Relational Database Management System (RDBMS) was developed and marketed by the Wang Corporation.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Packet	is a logical grouping of information that includes a header containing control information and (usually) user data. The term “packets” most often refers to network layer units of data.
Packet switching	is the process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets.
Paradox®	is a PC-based relational database management system (RDBMS) that supports SQL access and ODBC connectivity.
PARIS	an acronym for the Planning Application for Reporting Information Technology Strategy, a web-based application for use in preparing the budget unit IT plan for evaluation/approval by GITA in accordance with A.R.S. 41-3504A.1.(f). All components of the IT plan are entered into the PARIS application for submission to GITA by September 1 of each year.
Pascal	is a third-generation language (3GL) with a one-pass compiler. Designed for instructional purposes about 1967-68 by Nicholas Wirth, Pascal requires a programmer to define all routines and variables fully, including the nature of their use, before using them. While commercial versions of Pascal have been made available, it has had limited success in the business world.
Password Authentication Protocol (PAP)	is the authentication protocol that allows Point-to-Point Protocol (PPP) peers to authenticate one another. The remote router attempting to connect to the local router is required to send an authentication request. Unlike Challenge Handshake Authentication Protocol (CHAP), PAP passes the password and the host name or username in the clear (unencrypted). PAP does not itself prevent unauthorized access but merely identifies the remote end. The router or access server then determines whether that user is allowed access. PAP is supported only on PPP lines.
Patch	is a piece of software code inserted into a program to temporarily fix a defect. Patches are developed by software and equipment vendors to address vulnerabilities as they are discovered.
Patch management	is the process of effectively applying available patches to protect vulnerable hardware and software.
PC/SC	is an industry workgroup that develops smart card specifications that are completely platform independent, and can be implemented on any operating system. PC/SC work builds upon existing industry smart card standards - ISO7816 and EMV (Europay, MasterCard, and Visa) - and complements them by defining low-level device interfaces and device-independent application APIs as well as resource management, to allow multiple applications to share smart card devices attached to a system.
Personal Digital Assistants (PDAs)	are consumer electronic devices ranging from palm-held personal information managers to palm-held PCs.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
PL/I	is a third-generation (3GL) programming language developed in the early 1960s as an alternative to assembler language (for low-level computer processing functions), COBOL (for large-scale business applications), and FORTRAN (for scientific and algorithmic applications). PL/I stands for "Programming Language 1." PL/I was an antecedent of the C programming language, which essentially replaced it as an all-purpose programming language.
Plain Old Telephone Service (POTS)	is a general term referring to the variety of telephone (voice-only) networks and services in place worldwide.
Platform	is an underlying computer (device) system (hardware and software) on which application programs can run.
Point-to-Point Protocol (PPP)	is the successor to SLIP that provides router-to-router and host-to-network connections over synchronous and asynchronous circuits. Whereas SLIP was designed to work with IP, PPP was designed to work with several network layer protocols, such as IP and IPX. PPP also has built-in security mechanisms, such as CHAP and PAP. PPP relies on two protocols: LCP and NCP.
Policy	is any general statement of direction and purpose designed to promote the coordinated planning, practical acquisition, effective development, and efficient use of information technology resources.
Policy Authority	is the Arizona Secretary of State acting as the authoritative party designated in Statute (A.R.S. § 41-121 and A.R.S. § 41-132) and Administrative Rules for Electronic Signatures to establish policies and procedures for the use of electronic and digital signatures.
Policy, Standards, and Procedures program (PSP)	is the set of policies, standards, procedures and other documents which provide statewide direction for the approved methods of satisfying the GITA charter (A. R. S. § 41-3504).
Policy, Statewide	refers to a set of IT practices and rules that a State agency should use to manage, protect, and allocate its information resources. These Policies provide IT directives and expectations to establish goals and performance measures as established by emerging technologies and agency IT plans. They are intended to be high-level, and comprehensive enough (in terms of technical direction and best practices) to satisfy the needs of the State agencies, but not so detailed whereby consensus cannot be achieved. Budget units should comply with the goals and objectives of the State of Arizona, as prescribe by A. R. S. § 41-3504, unless identified by exception.
Portability	is 1. The ability to transfer data from one system to another without being required to recreate or reenter data descriptions or to modify significantly the application being transported. 2. The ability of software or of a system to run on more than one type or size of computer under more than one operating system. Note: An application is portable across a class of environments to the degree that the effort required to transport and adapt it to a new environment in the class is less than the effort of redevelopment.
Portable Document Format (PDF)	is a non-editable file format that captures all the elements of a printed document as an electronic image that a user is able to view, navigate, print, or forward to another user.

Keyword	Description
Portable Network Graphics (PNG)	is a file format for image compression that, in time, is expected to replace the Graphics Interchange Format (GIF) that is widely used on the Internet. The PNG format was developed by an Internet committee expressly to be patent-free and provide a number of improvements over the GIF format.
Portable Operating System Interface (POSIX)	is a set of standard operating system interfaces based on the UNIX operating system. The need for standardization arose because enterprises using computers wanted to be able to develop programs that could be moved among different manufacturers' computer systems without having to be recoded. UNIX was selected as the basis for a standard system interface partly because it was "manufacturer-neutral." However, several major versions of UNIX existed so there was a need to develop a common-denominator system.
Post Office Protocol 3 (POP3)	is the most recent version of a standard protocol for receiving email. POP3 is a client/server protocol in which email is received and held for a user by an Internet server.
Postscript	is a format used to create and send documents over the Internet. Postscript by Adobe Systems, Inc., is the standard page description and printer language for desktop computer systems. It describes type, graphics, and halftones, as well as the placement of each on the page.
PowerBuilder®	is a rapid application development (RAD) tool for building object-oriented programming applications. A major feature of PowerBuilder® (and its competitors) is the ability to create databases using an object-oriented interface. Applications created with PowerBuilder® can access other popular types of databases on other major platforms using Open Database Connectivity (ODBC).
Pretty Good Privacy (PGP)	refers to a non-PKI implementation of asymmetric cryptography that recognizes PGPTM certificates and X.509 (PKI) certificates. PGPTM is an acceptable technology for electronic signatures, message integrity, sender authentication, and encryption. PGP-based technical functionality defined the current, open standard, known, as the Open Specification for PGPTM, is an evolving definition developed by the IETF through their OpenPGP working group. PGPTM is only appropriate for very small, closed communities that have agreed to recognize the use of PGPTM in that community. The use of PGPTM for electronic signatures requires the encapsulation of the message in such a way that altering the message invalidates the signature. The Policy Authority defines the particular policy and processes required. The signing process also assures the message integrity and sender authentication. PGPTM provides a medium level of confidence that a signed document is intact and authentic

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Pretty Good Privacy (PGP) Certificate	refers to an electronic record, which includes (but is not limited to): 1. The PGPTM version number, which identifies which version of PGPTM, was used to create the key associated with the certificate. 2. The certificate holder's public key, which is the public portion of the subscriber's key pair, together with the algorithm of the key: i.e., RSA, DSS, or ECC. 3. The certificate holder's information, which consists of "identity" information about the user, such as his or her name, user ID, photograph, and so on. 4. The digital signature of the certificate owner, also called a self-signature. This is the signature using the corresponding private key to the public key associated with the certificate. 5. The certificate's validity period, which is the certificate's start date/time and expiration date/time? 6. The preferred symmetric encryption algorithm for the key, which indicates the encryption algorithm to which the certificate owner prefers to have information encrypted. The supported algorithms include IDEA or 3DES. 7. Conformance to IETF OpenPGP standards.
Private Branch Exchange (PBX)	is a customer-site telephone switching system.
Private Key	refers to the privately held key of a key pair used to create a digital signature or to un-encrypt an encrypted message or file.
Procedure	is instructions describing how to achieve the policy or standard. A procedure establishes and defines the process, whereby a budget unit complies with the policies of the State of Arizona, as prescribed by A.R.S. § 41-3504, unless identified by exception.
Productivity software	, in relation to Arizona's EWTA, includes office automation and collaborative software products and tools, sometimes referred to as "groupware," including email, calendaring and scheduling, office automation software with word processing, spreadsheet, presentation, graphic applications, etc.
Programming languages	are a formal system of signs and symbols (as COBOL or a calculus in logic) including rules for the formation and transformation of admissible expressions into the set of symbolic instruction codes usually in binary form that is used to represent operations and data in a machine (as a computer). Programming languages have evolved through several major steps or "generations" which include: 1. First-generation language (1GL) is machine language or the level of instructions and data that the processor is actually given to work on (which in conventional computers is a string of 0s and 1s). 2. Second-generation language (2GL) is assembler (sometimes called "assembly") language. An assembler converts the assembler language statements into machine language. 3. Third-generation language (3 GL) is a "high-level" programming language, such as COBOL, C, or Java™. A compiler converts the statements of a specific high-level programming language into machine language. 4. Fourth-generation language (4GL) is designed to be closer to natural language than a 3GL language. Languages for accessing databases, such as SQL, are often described as 4GLs. 5. Fifth-generation language (5GL) is programming that uses a visual or graphical development interface to create source language that is usually compiled with a 3GL or 4GL language compiler.
Programming Software	, also referred to as "Application Development Software," are enabling technologies and products used to develop and maintain Software Applications and include programming languages (COBOL, C++, Java™, HTML, etc.), middleware, report writers, etc.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Programs	are a specific set of ordered operations for a device to perform. Programs are created using a programming (computer) language. The language statements are referred to as the source program. The source program is "compiled" (with a special program called a language compiler) and the result is called an object program or object code (not to be confused with object-oriented programming.) The object program contains the string of 0s and 1s called machine language that the logic processor works with. The machine language of the computer is constructed by the language compiler with an understanding of the computer's logic architecture, including the set of possible computer instructions and the length (number of bits) in an instruction.
Progress®	is both a relational database management system (RDBMS) and an application development environment. Progress® provides for a variety of platforms and operating systems, XML and SOAP. Progress® implements a standards-based approach to application integration that is flexible, cost-effective, scalable, and open.
Project	is a specific series of activities and events involving the implementation of new or enhanced IT systems of $25,000 or more in development costs over a prescribed period, not greater than 5 years.
Project and Investment Justification (PIJ)	is a statewide standard document that Budget Units use to describe planned IT projects and investments. It identifies all resources, technologies, benefits, costs, goals, and risks associated with the project. The document establishes a specific time period for the project or investment.
Protocol	is the formal description of a set of rules and conventions that govern how devices on a network exchange information.
Protocol Independent Multicast (PIM)	is multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: dense and sparse.
Proxy servers	are intermediary programs that act as both a server and a client for making requests on behalf of other clients. Requests are serviced internally or by passing them on, possibly after translation, to other servers. A proxy interprets, and, if necessary, rewrites a request message before forwarding it.
PSP Document Owner	is the GITA manager or leader who is responsible for the implementation of the PSP document.
Public / private key cryptography	is a form of cryptography using two related keys. Information encrypted with one key can only be decrypted with the other key. The `Public' Key is made openly available in a repository to anyone who wants to communicate with the user in a secure manner. The `Private' Key is kept only by the owner and is never divulged. Since only the owner has the private key, its use is considered sufficient to uniquely authenticate the owner. A PKI-based electronic signature is formed when a message digest is created for the entirety of a message with the legal intent of being a signature affixed to the message.
Public domain	refers to property rights that are held by the public at large regarding material that exists without copyright protection.
Public key	refers to the public key of a key pair used to verify a digital signature or to encrypt a message or file.

Keyword	Description
Public key certificate	(also known as an X.509 Certificate) is an electronic record, which identifies the Certification Authority issuing it, names or identifies its subscriber, contains the subscriber's public key, is electronically signed by the certification authority issuing it, and conforms to X.509/PKIX standards.
Public Key Infrastructure (PKI)	is a collection of certificates, with their issuing CA's, subjects, relying parties, RA's, and repositories. PKI is a system of Certificate Authorities that perform some set of certificate management, archive management, key management, and token management functions for a community of users in an application of asymmetric cryptography. PKI is an acceptable technology for electronic signatures, sender authentication, message integrity, and encryption. PKI-based technical functionality is defined by Standard X.509 version 3 (or a succeeding version adopted by the Internet Engineering Task Force (IETF) as incorporated into PKIX by the Standards Development Task Group. The use of PKI for electronic signatures requires the encapsulation of the message in such a way that altering the message invalidates the electronic signature. The Policy Authority defines the particular policy and processes required. The signing process also assures the message integrity and sender authentication.
Public Switched Telephone Network (PSTN)	is the world's collection of interconnected voice-oriented public telephone networks, both commercial and government-owned. It is also referred to as the Plain Old Telephone Service (POTS).
Quality of Service (QoS)	is the concept that transmission rates, error rates, and other characteristics can be measured, improved, and, to some extent, guaranteed in advance. QoS is of particular concern for the continuous transmission of high-bandwidth video and multimedia information. Transmitting this kind of content dependably is difficult in public networks using ordinary "best effort" protocols. Using the Internet's Resource Reservation Protocol (RSVP), packets passing through a gateway host can be expedited based on policy and reservation criteria arranged in advance.
Rapid Application Development (RAD)	is a concept that products can be developed faster and of higher quality through: 1. Gathering requirements using workshops or focus groups; 2. Prototyping and early, reiterative user testing of designs; 3. The re-use of software components; 4. A rigidly paced schedule that defers design improvements to the next product version; and 5. Less formality in reviews and other team communication. Some companies offer products that provide some or all of the tools for RAD software development. These products include requirements gathering tools, prototyping tools, computer-aided software engineering tools, language development environments such as those for the Java™ platform, groupware for communication among development members, and testing tools. RAD usually embraces object-oriented programming methodology, which inherently fosters software re-use. The most popular object-oriented programming languages, C++ and Java™, are offered in visual programming packages often described as providing rapid application development.
Realm Specific IP (RSIP)	(RFC 3103) is an experimental protocol that allows negotiation of resources between an RSIP host and gateway so that the host can lease some of the gateway's addressing parameters in order to establish a global network presence. This protocol is designed to operate on the application layer and to use its own TCP or UDP port. In particular, the protocol allows a gateway to allocate addressing and control parameters to a host such that a flow policy can be enforced at the gateway.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Real-Time Streaming Protocol (RTSP)	is an application-level protocol for control over the delivery of data with real-time properties. RTSP provides an extensible framework to enable controlled, on-demand delivery of real-time data, such as audio and video. Sources of data can include both live data feeds and stored clips. This protocol is intended to control multiple data delivery sessions, provide a means for choosing delivery channels such as UDP, multicast UDP and TCP, and provide a means for choosing delivery mechanisms based upon RTSP (IETF RFC 1889).
Real-Time Transport Protocol (RTP)	is an Internet protocol standard that specifies a way for programs to manage the real-time transmission of multimedia data over either unicast or multicast network services. Originally specified in Internet Engineering Task Force (IETF) Request for Comments (RFC) 1889, RTP was designed by the IETF's Audio-Video Transport Working Group to support video conferences with multiple, geographically dispersed participants. RTP is commonly used in Internet telephony applications. RTP does not in itself guarantee real-time delivery of multimedia data (since this is dependent on network characteristics); it does, however, provide the wherewithal to manage the data as it arrives to best effect. RTP combines its data transport with a control protocol (RTCP), which makes it possible to monitor data delivery for large multicast networks. Monitoring allows the receiver to detect if there is any packet loss and to compensate for any delay jitter. Both protocols work independently of the underlying Transport layer and Network layer protocols. Information in the RTP header tells the receiver how to reconstruct the data and describes how the codec bit streams are packetized. As a rule, RTP runs on top of the User Datagram Protocol (UDP), although it can use other transport protocols. Both the Session Initiation Protocol (SIP) and H.323 use RTP.
Redundant Array of Independent Disks (RAID)	is a disk array in which part of the physical storage capacity is used to store redundant information about user data stored on the remainder of the storage capacity. The redundant information enables regeneration of user data in the event that one of the array's member disks or the access path to it fails. There are a number of RAID levels, each of which provides a different amount of redundancy and performance.
Relational Database Management System (RDBMS)	is a set of computer programs with a user and/or programming interface that supports the definition of the format of a relational database, and the creation of and access to its data. A database management system removes the need for a user or program to manage low-level database storage. It also provides security for and assures the integrity of the data it contains.
Relational databases	are collections of data items organized as a set of formally described tables from which data can be accessed or reassembled in many different ways without having to reorganize the database tables. The standard user and application program interface to a relational database is the Structured Query Language (SQL). SQL statements are used both for interactive queries for information from a relational database and for gathering data for reports.
Relying party	refers to means the party receiving the message incorporating an electronic signature and relying on it to authenticate the signer and that the message has not been altered.

Keyword	Description
Remote Authentication Dial-In User Service (RADIUS)	is a database for authenticating modem and other external connections and for tracking connection time. RADIUS is a distributed client/server system that secures networks against unauthorized access. RADIUS clients run on boundary routers and send authentication requests to a central RADIUS server that contains all user authentication and network service access information. RADIUS is a fully open protocol, distributed in source code format that can be modified to work with any security system currently available on the market.
Remote Method Invocation (RMI)	is a method, using the Java™ programming language and development environment, to write object-oriented programming in which objects on different devices can interact in a distributed network. RMI is the Java™ version of what is generally known as a Remote Procedure Call (RPC), but with the ability to pass one or more objects along with the request. The object can include information that will change the service that is performed in the remote device.
Remote Network Monitoring (RMON)	, defined by RFC1757, provides extensions to the Simple Network Management Protocol (SNMP) that provide comprehensive network monitoring capabilities. Standard SNMP is designed so that the device being monitored has to be queried to obtain information. RMON is proactive so it eliminates the polling required in standard SNMP: it can set alarms on a variety of traffic conditions, including specific types of errors. The full RMON capabilities are very extensive so routers and other network devices generally only implement portions of it. RMON2 extensions to RMON that include: potocol directory (identifies packets used by many of the new groups in the standard), protocol distribution (counts of traffic per protocol), address mapping (MAC addresses), network layer host (tracks amount of traffic between network addresses), network layer matrix (determines top conversations between network addresses), application layer host (tracks amount of traffic by application protocol), and application layer matrix (information on top conversations based on application protocols). RMON2 has better traffic analysis capabilities than RMON, but not all network devices implement the standard and it requires much more processor bandwidth than RMON.
Remote Procedure Call (RPC)	is a protocol that one program can use to request a service from another program located in another computer in a network without having to understand network details. (A procedure call is also sometimes known as a function call or a subroutine call.) RPC uses the client/server model. The requesting program is a client and the service-providing program is the server. Like a regular or local procedure call, an RPC is a synchronous operation requiring the requesting program to be suspended until the results of the remote procedure are returned. However, the use of lightweight processes or threads that share the same address space allows multiple RPCs to be performed concurrently. The IEEE defines RPC in its Remote Procedure Call Specification, ISO/IEC CD 11578 N6561.
Report Program Generator (RPG)	is a programming language that originated as a report-building program and evolved into a fully procedural programming language. Its latest version, RPG IV, provides for SQL and XML functionality. Historically, RPG has probably been the second most used programming language, after COBOL, for commercial applications on mid-range computers.

Keyword	Description
Report writers	, also referred to as report generation programs, allow for the creation of reports from a variety of data sources with a minimum of written code. Report writers generally can access data from most widely used databases and can integrate data from multiple databases within one report using Open Database Connectivity (ODBC).
Repositories	contain detailed information about the data that is stored in a data warehouse (i.e., metadata). A repository is an important component of the data warehouse because it represents the shared understanding of data. A repository typically stores the following information: 1. Data definitions for the data stored in the data warehouse database. 2. Aliases that can be used to reference the data. 3. Data structures. 4. Systems where the original data is found, including the format of the original data. 5. Processes used to extract the data from the original location. 6. Sources of record for the data. A source of record is an authoritative source for data, where data in a source of record is trusted to be accurate and up-to-date. The original data and the source of record may be the same. 7. Systems and processes using the data. If changes are made that may affect systems and users using the data, it is important to keep this type of information in the repository.
Repository Authority (RA)	refers to the party that validates status of a public key for a relying party. It is generally an online source of up-to-date information about certificates, their current reliability, and other related information.
Repository management systems	store and manage the metadata and information model for a data warehouse. The repository must be actively maintained (e.g., changes to metadata occur in the repository before the changes occur in the data warehouse). The repository serves as a primary data warehouse administration tool and helps promote data reusability, reliability, and sharing across the enterprise. The repository management system should be the same used by the federated data information repository and should support multiple types of data elements.
Repudiation	is the denial by one of the entities involved in a communication of having participated in all or part of the communication.
Request for Comments (RFC)	is a formal document from the Internet Engineering Task Force (IETF) that is the result of committee drafting and subsequent review by interested parties. Some RFCs are informational in nature. Of those that are intended to become Internet standards, the final version of the RFC becomes the standard and no further comments or changes are permitted. Change can occur, however, through subsequent RFCs that supersede or elaborate on all or parts of previous RFCs.
Resource Description Framework (RDF)	is a general framework for how to describe any Internet resource such as a Web site and its content. An RDF description (such descriptions are often referred to as metadata, or "data about data") can include the authors of the resource, date of creation or updating, the organization of the pages on a site (the sitemap), information that describes content in terms of audience or content rating, key words for search engine data collection, subject categories, and so forth. RDF will make it possible for everyone to share Web site and other descriptions more easily and for software developers to build products that can use the metadata to provide better search engines and directories, to act as intelligent agents, and to give Web users more control of what they are viewing. RDF is an application of another technology, the Extensible Markup Language (XML), and is being developed under the auspices of the World Wide Consortium (W3C).

Keyword	Description
Resource Reservation Protocol (RSVP)	is a means for reserving network resources—primarily bandwidth—to guarantee that applications transmitting end-to-end across the Internet will perform at the desired speed and quality. RSVP is an IP service that allows end systems or hosts on either side of a router network to establish a reserved-bandwidth path between them to predetermine and ensure QoS for their data transmission. Based on IETF RFC2205: a resource reservation setup protocol for IP networks that is being implemented by 802.1p and ATM. Routers can use RSVP-based signaling exchanges to reserve or set aside resources such as bandwidth that may be needed to handle designated traffic flows. RSVP is the protocol that is proposed for distributing MPLS (Multi-Protocol Label Switching) data to routers.
Rich Text Format (RTF)	is a file format that allows the exchange of text files between different word processing software in different operating systems. The RTF Specification uses a variety of industry-wide character sets and defines control words and symbols that serve as "common denominator" formatting commands. When saving a file in the Rich Text Format, an RTF writer that converts the word processor's markup to the RTF language processes the file. When being read, an RTF reader that converts the RTF language into formatting for the word processor that will display the document processes the control words, and symbols.
Ring topology	is a connection of two or more stations in a logically circular configuration. Information is passed sequentially between active stations. Token Ring and FDDI are based on this topology.
Rivest-Shamir-Adleman (RSA)	is the most commonly used Internet encryption and authentication algorithm system, and is included as part of the Web browsers from major manufacturers.
Role-based administration	is a security administration practice that assigns rights and permissions based on performance of a particular function (using a pre-defined "group") rather than on an individual basis.
Router	is a LAN/WAN device operating at Layers 1 (physical), 2 (data link), and 3 (network) of the OSI 7 Layer Reference Model.
Routing Information Protocol (RIP)	is used to monitor the state of the links that interconnect routers within a network, or with other networks.
Satellite communication	is the use of orbiting satellites to transmit information between multiple, earth-based stations.
Scalability	is the ability of a software application or product (hardware or software) to continue to function as originally arranged and constructed, and to retain performance levels as it (or its context) is changed in size or volume in order to meet a user need. Ideally, It is the ability not only to function as originally arranged and constructed in the rescaled situation, but also to actually take full advantage of it.
Secret key technology	(also known as symmetric encryption) is a form of cryptography where encryption and decryption use the same key. Pairs of users or processes share the same secret key. Data encrypted with a secret key is decrypted using the same key. Secret key technology is used to do most encryption because it is much faster than other techniques. Examples of commonly used secret key algorithms include 3DES and IDEA.

Keyword	Description
Secure Multi-Purpose Internet Mail Extensions (S/MIME)	is a secure method of sending email that uses the Rivest-Shamir-Adleman (RSA) encryption system. Vendors that make messaging products have endorsed S/MIME. RSA has proposed S/MIME as a standard to the Internet Engineering Task Force (IETF). An alternative to S/MIME is PGP/MIME, which has also been proposed as a standard.
Secure Socket Shell (SSH)	is a protocol that provides a secure remote connection to an internetworking device or remote computer through a Transmission Control Protocol (TCP) application.
Secure Sockets Layer (SSL)	is an application-level protocol that enables secure transactions of data by ensuring privacy, authentication, and data integrity. It relies upon certificates, public keys, and private keys.
Security Assertion Markup Language (SAML)	is an Extensible Markup Language (XML) standard that allows a user to log on once for affiliated but separate web sites. SAML is designed for business-to-business and business-to-consumer transactions. SAML specifies three components: assertions (authentication, attribute, and authorization), protocol, and binding. Authentication assertion validates the user's identity. Attribute assertion contains specific information about the user. Authorization assertion identifies what the user is authorized to do.
Security tokens	are physical cards similar to credit cards that work in conjunction with a user ID to identify a user to the system. They combine something a person knows, such as a password or PIN, with something they possess, a token card. Token cards commonly generate either dynamic passwords or a response in a challenge-response communication between the user and the system.
Segment	is the term used in the TCP specification to describe a single transport layer unit of information. A segment is also a section of a network that is bounded by bridges, routers, or switches.
Sensitive information	refers to any confidential or critical information for which the loss, misuse, or unauthorized access to or modification or improper disclosure and could adversely affect the State of Arizona's interest, the conduct of Agency programs, or the privacy to which individuals are entitled.
Sequenced Packet Exchange (SPX)	is a connection-oriented NetWare protocol that supplements the datagram service provided by OSI network layer (Layer 3) protocols.
Serial Line Internet Protocol (SLIP)	was the standard protocol for point-to-point serial connections using a variation of TCP/IP. SLIP was the predecessor of PPP.
Server Message Block (SMB)	is a file-system protocol used in network operating systems to package data and exchange information with other systems. The SMB protocol provides a method for client applications in a computer to read and write to files on and to request services from server programs in a network. The SMB protocol can be used over the Internet on top of its TCP/IP protocol or on top of other network protocols. Using the SMB protocol, an application, (or the user of an application) can access files at a remote server as well as other resources. Thus, a client application can read, create, and update files on the remote server. It can also communicate with any server program that is set up to receive an SMB client request.

Keyword	Description
Servlets	are small software programs that run on server devices. The term was coined in the context of the Java™ applet, which is a small software program that is sent as a separate file along with a Web (HTML) page. Java™ applets, usually intended for executing on a client device, can result in such services as performing a calculation or positioning an image based on an end-user interaction.
Session Announcement Protocol (SAP)	is a multicast session directory announcement protocol designed to assist the advertisement of multicast multimedia conferences and other multicast sessions, and to communicate the relevant session setup information to prospective participants. A distributed session directory may be used.
Session Description Protocol (SDP)	is an application-layer control protocol for describing multimedia sessions for the purposes of session announcement, session invitation, and other forms of multimedia session initiation. SDP is intended to be general purpose so that it can be used for a wider range of network environments and applications than just multicast session directories.
Session Initiation Protocol (SIP)	is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. Sessions include Internet multimedia conferencing, telephony, presence, event notification, and instant messaging. SIP was developed within the IETF MMUSIC (Multiparty Multimedia Session Control) working group, with work proceeding since September 1999 in the IETF SIP working group. SIP transparently supports name mapping and redirection services, allowing the implementation of intelligent network telephony subscriber services. These facilities also enable personal mobility, which is the ability of end users to originate and receive calls and access subscribed telecommunication services on any terminal in any location, and the ability of the network to identify end users as they move. Personal mobility is based on the use of a unique personal identity (i.e., personal number). Personal mobility complements terminal mobility, which is the ability to maintain communications when moving a single end system from one subnet to another.
Shall	identifies required activities. “Shall” directs that alternatives are not acceptable without formal approval of the State CIO.
Shielded Twisted Pair (STP)	is a twisted-pair wire with jacket shielding, used for long distances. It is less subject to electrical noise and interference than UTP.
Should	Identifies recommended, but not required, activities
Simple API for XML (SAX)	is an application program interface (API) that allows a programmer to interpret a Web file that uses the Extensible Markup Language (XML) - that is, a Web file that describes a collection of data. SAX is an alternative to using the Document Object Model (DOM) to interpret the XML file. As its name suggests, it's a simpler interface than DOM and is appropriate where many or very large files are to be processed, but it contains fewer capabilities for manipulating the data content.
Simple Mail Transfer Protocol (SMTP)	is a TCP/IP protocol used in sending and receiving email. Since SMTP is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP that let the user save messages in a server mailbox and download them periodically from the server. SMTP is usually implemented to operate over TCP port 25. SMTP details are included in IETF RFC 821.

Keyword	Description
Simple Network Management Protocol (SNMP)	is a set of network communication specifications that cover all the basics of network management. It is a simple and expandable protocol designed to give the capability to remotely manage a computer network by polling, setting terminal values, and monitoring network events. It is comprised of three elements; a management information base, a manager, and the agents. The manager is located on the host computer on the network. Its role is to poll the agents and request information concerning the network's status. Agents run off each network node and collect network and terminal information as specified in the MIB.
Simple Object Access Protocol (SOAP)	provides a simple and lightweight mechanism for exchanging structured and typed information between peers in a decentralized, distributed environment using XML. SOAP defines a simple mechanism for expressing application semantics by providing a modular packaging model and encoding mechanisms for encoding data within modules. This allows SOAP to be used in a large variety of systems ranging from messaging systems to RPC. Where XML allows very flexible encoding of data, SOAP defines a narrower set of rules for encoding.
Simple Object Access Protocol (SOAP) with Attachments API for Java (SAAJ)	enables developers to produce and consume messages conforming to the SOAP specification and SOAP with Attachments note.
Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs) (STUN)	(RFC 3489) is a lightweight protocol that allows applications to discover the presence and types of NATs and firewalls between them and the public Internet. It also provides the ability for applications to determine the public Internet Protocol (IP) addresses allocated to them by the NAT. STUN does not work with symmetric NATs.
Single-Mode Optical Fiber (SMF)	has a single propagation path for light. It is typically used for higher speeds or longer distances (as compared to multimode optical fiber).
SIP for Instant Messaging and Presence Leveraging Extensions (SIMPLE)	is an add-on to the Session Initiation Protocol (SIP) that some industry insiders predict will be the basis for a new Instant Messaging and Presence Protocol (IMPP).
Small Computer Systems Interface (SCSI)	is a collection of ANSI interface standards for host computers communicating with attached peripherals. Initially associated with a parallel bus interface, today SCSI also supports serial networked interfaces for connection across Fiber Channel and Gigabit Ethernet (iSCSI).
Small Computer Systems Interface (SCSI) over IP (iSCSI)	is the encapsulating of existing protocols, such as SCSI and Fiber Channel, in an IP-based transport or transports. The IETF working group is focusing on the transport or transports and related issues (e.g., security, naming, discovery, and configuration), as opposed to modifying existing protocols. Standards for the protocols to be encapsulated are controlled by other standards organizations (e.g., NIST T10 [SCSI] and T11 [Fiber Channel]) for accessing block-level storage from IP-connected hosts. With iSCSI, SCSI commands and data frames are encapsulated in IP to support IP-connected server to storage I/O disk access communication across IP networks.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Smalltalk	is a programming language that was designed expressly to support the concepts of object-oriented programming. In the early 1970's, Alan Kay led a team of researchers at Xerox to invent a language that let programmers envision the data objects they intended to manipulate. Unlike C++, Smalltalk was not built on the syntax of a procedural language; it is a "pure" object-oriented language with more rigorously enforced rules than C++, which permits some of the procedural constructs of the C language. Although Smalltalk may continue to attract a loyal following, Java™, a derivative of C++ designed for distributed systems, has become the most prevalent object-oriented language on the Web.
Smart cards	are a tamper-resistant computer embedded in a credit-card-sized device. The cards have embedded integrated circuits that implement a CPU, application data storage, and RAM used by the CPU. A smart card and associated host software are used both as an application platform and as an identification and authentication device. Identification security for smart cards is based on the user physically having the smart card, the user knowing a password or PIN to activate the card's functions, the security functions available on the cards, and the tamper-resistant qualities of the card.
Social engineering	is a practice that can be used to exploit what has long been considered the 'weakest link' in the security chain of an organization - the 'human factor.' Social engineering can be regarded as 'people-hacking' for soliciting unwitting participation from a person inside a company rather than breaking into the system independently.
Speaker Verification API (SVAPI)	is an API used for incorporating speaker-recognition technology into desktop and network applications. SVAPI offers interoperability over distributed environments with related APIs.
Sphere of influence	is defined as all those activities controlled within the confines of each agency and any additional responsibilities as designated in statute or rule.
SPMO	is the Arizona Department of Administration, Management Services Division, and Surplus Property Management Office.
SPO	is the Arizona Department of Administration, State Procurement Office.
Spyware	is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties. Spyware can get in a computer as a software virus or as the result of installing a new program. Data collecting programs that are installed with the user's knowledge are not, properly speaking, spyware, if the user fully understands what data is being collected and with whom it is being shared.
SQLJ	is a set of programming extensions that allow a programmer using the Java programming language to embed statements that provide SQL (Structured Query Language) database requests. SQLJ is similar to existing extensions for SQL that are provided for C, Formula Translation, and other programming languages. SQLJ is being proposed as a standard and a simpler and easier-to-use alternative to Java Database Connectivity (JDBC).
Standard	is a directive or specification whose compliance is mandatory, and whose implementation is deemed achievable, measurable, and auditable for compliance.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Standard Generalized Markup Language (SGML)	is a language for describing markup languages, particularly those used in electronic document exchange, document management, and document publishing. HTML is an example of a language defined in SGML.
Standard, Statewide	, Statewide is a mandatory statement of direction on products and/or services to be used by State agencies. In keeping with fair competition laws, statewide standards shall also be high level, and comprehensive enough with facts and features in defining minimum and acceptable IT requirements. Budget Units should comply with the policies of the State of Arizona, as prescribed by A.R.S. § 41-3504, unless identified by exception.
Star topology	is a topology in which end points on a network are connected to a common central switch by point-to-point links. A ring topology that is organized as a star implements a unidirectional closed-loop, instead of point-to-point links.
State Information Protection Center (SIPC)	is a function of ADOA ISD Security Services that creates or receives computer security alerts and forwards them to all Agency CIOs and/or Agency SIPC Coordinators. Conversely, SIPC also collects incident notifications from agencies that detect cyber intrusions.
State Library, Archives and Public Records (SLAPR) or (DLAPR)	serves the information needs of Arizona citizens as authorized in Arizona Revised Statutes §41-1331 through §41-1352. Through its divisions, the Agency provides access to unique historical and contemporary resources.
Static Content	is information contained on a web page that remains the same every time a viewer accesses it. Static content is coded directly into the HTML page and does not require sophisticated programming or database support.
Storage Area Network (SAN)	defines the hardware and software associated with enabling block-level data transfer between storage devices and hosts in a networked paradigm. Today, the predominant SAN technology is Fiber Channel however, with the creation of iSCSI a combination of fiber channel and gigabit Ethernet technologies to form the infrastructure for SANs is possible in the future.
Storage networking	is the practice of creating, installing, administering, or using networks whose primary purpose is the transfer of data between computer systems and storage elements and among storage elements.
Strategic	also referred to as “Target” is one of four categories used in the PSP program and EA to guide technology use in the State of Arizona (see also emerging, obsolescent, and transitional). “Strategic” implies that the State’s Enterprise Architecture promotes use of this technology by agencies. New deployments of this technology are recommended.
Structured Query Language (SQL)	is a standard interactive and programming language for getting information from and updating a database. Although SQL is both an ANSI and an ISO standard, many database products support SQL with proprietary extensions to the standard language.
Subscriber	refers to a person who is the subject listed in a PGPTM or PKI certificate, accepts his or her own certificate, and holds a private key which corresponds to a public key listed in that certificate.
Superbase	is a PC-based relational Database Management System (RDBMS) that supports SQL access and ODBC connectivity.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Switch	is a circuit switching device. Switching is a communications paradigm in which a dedicated communication path is established between the sender and receiver along which all packets travel.
Switched Multimegabit Data Services (SMDS)	is a high-speed, packet-switched, datagram-based WAN networking technology offered by the public carriers.
Switching	is a communications paradigm in which a dedicated communications path is established between a sender and receiver along which all data packets travel.
Sybase	product families include databases, development tools, integration middleware, enterprise portals, and mobile and wireless servers. Sybase relational database management system (RDBMS) software is a data management platform designed for transaction-intensive enterprise applications, with advanced capabilities to meet the evolving requirements of e-Business. Sybase databases provide support for Extensible Markup Language (XML) and Unicode data, Java™ classes and objects, and Enterprise JavaBean™ (EJB™) components
Symmetric-key cryptography	is a cryptographic system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Symmetric-key systems are simple and fast, but their main drawback is that the two parties must somehow exchange the key in a secure way. Symmetric-key cryptography is sometimes called secret-key cryptography.
Synchronous	software program-to-program communication requires that each end of an exchange of communication respond in turn without initiating a new communication. A typical activity that might use a synchronous protocol would be a transmission of files from one point to another. As each transmission is received, a response is returned indicating success or the need to resend. Each successive transmission of data requires a response to the previous transmission before a new one can be initiated.
Synchronous Data Link Control (SDLC)	is a bit-oriented, protocol, de-facto standard that does not support the extended address field or the extended control field.
Synchronous Optical Network (SONET)	is a United States standard for fiber-optic digital hierarchy (speeds range from 51.84 Mbps to 9.953 Gbps) that includes all aspects of transporting and managing digital traffic over fiber-optic facilities in the public network.
Systems	are a collection of elements or components that are organized for a common purpose. The word may describe the organization or plan itself, and may also describe the parts in the system (as in "computer system").
Systems Network Architecture (SNA)	is a large, complex, feature-rich network architecture developed in the 1970s by IBM.
T1	is a term for a digital carrier facility used to transmit a DS1-formatted digital signal at 1.544 megabits per second or a 24-analog-line equivalent.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Tag Image File Format (TIFF)	is a common, industry-wide file format for exchanging raster graphics (Raster graphics are digital images created or captured as a set of samples of a given space). A raster is a grid of X & Y coordinates on a display space -- and for three-dimensional images, a Z coordinate. A raster image file identifies which of these coordinates to illuminate in monochrome or color values. The raster file is sometimes referred to as a bitmap because it contains information that is directly mapped to the display (grid) images between software programs, including those used for scanned images.
Target Platform Architecture Assessment	is the formal application of specific requirements for the versatility, operating systems, security, and open standard interfaces/drivers that define target platform technologies to a particular device being used in the State or considered for use.
Technology	is defined as the application of science, especially to industrial or commercial objectives. It is the scientific method and material used to achieve a commercial or industrial objective. Technology is commonly thought of as electronic or digital products and systems considered as a group. Historically, it is the body of knowledge available to a society that is of use in fashioning implements, practicing manual arts and skills, and extracting or collecting materials.
Telecommunication system	is system including, but not limited to, all instrumentalities, facilities, apparatuses and services, for the transmission and reception of messages, impressions, signs, pictures, sounds or any other symbols by wire, radio, optical cable, electromagnetic or other similar means.
Telnet	is a standard terminal emulation protocol in the TCP/IP protocol stack. Telnet is used for remote terminal connection, enabling users to log in to remote systems and use resources as if they were connected to a local system.
Terminal Access Control Access Control System (TACACS)	is an authentication protocol, developed by the DDN community, which provides remote access authentication and related services, such as event logging. User passwords are administered in a central database rather than in individual routers, providing an easily scalable network security solution.
Terminal emulation	is the ability to make a client device, typically a PC, appear to look like another client device, usually an older type of terminal, so that an end-user can access software applications originally written to communicate with the other terminal type.
Third-Party Hosting	is the use of an external service provider to supply storage, connectivity, and services associated with making web pages available to viewers.
Three (3)-tier client/server applications	, refer to Application Architecture Perspectives.
Time Division Multiple Access (TDMA)	is a type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval ("slot" or "slice") for the transmission of each channel, that is, the channels take turns using the link. Some kind of periodic synchronizing signal or distinguishing identifier usually is required so that the receiver can tell which channel is which.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Time-Division Multiplexing (TDM)	is a scheme in which numerous signals are combined for transmission on a single communications line or channel. Each signal is broken up into many segments, each having very short duration. The circuit that combines signals at the source (transmitting) end of a communications link is known as a multiplexer. It accepts the input from each individual end user, breaks each signal into segments, and assigns the segments to the composite signal in a rotating, repeating sequence. The composite signal thus contains data from all the end users. At the other end of the long-distance cable, the individual signals are separated out by means of a circuit called a demultiplexer, and routed to the proper end users. A two-way communications circuit requires a multiplexer/demultiplexer at each end of the long-distance, high-bandwidth cable.
Token	(or security token) is an item used in authentication by ownership that contains information about the individual requesting access. Possession of the token allows a network-attached device to transmit data onto a network.
Token ring	is an IEEE 802.5 standard for media access. Conflicts in the transmission of messages are avoided by the granting of "tokens" which give permission to send. Token Ring was developed and supported by IBM and runs at 4 or 16 Mbps over a ring topology.
Token-based authentication	uses security tokens that contain identification control information about the individual requesting access. Possession of the token allows a network device to transmit data onto the network.
Total life cycle costs	are the sum of vendor costs, total State costs and financing costs throughout the life cycle of the information systems or telecommunication systems being acquired or developed (ARS 41-2553). Another term used with the same meaning is Life Cycle Analysis.
Total State costs	are the costs to the State of the information systems or telecommunications systems including cost of energy, facilities, personnel and all other identifiable development costs (ARS 41-2553).
Transaction Processing Monitors (TPM)	are middleware products servicing clients requiring transaction services in an n-tier distributed application environment. TPM middleware products are important when applications require high transaction volumes, load balancing, failure recovery, and fail-over capabilities. Transaction Processing Monitors provide the following core services: #Transaction Integrity -- Necessary services to ensure those atomic database transactions comprising a business transaction are applied successfully or not at all. #Two-Phase Commit -- A means of implementing transaction integrity when there is more than one target database system (server) involved in the transaction. #Failure Recovery -- A means for reestablishing the appropriate connections and restarting transactions when network and platform outages occur. #Load Balancing -- A feature of transaction monitors in which the server component manages the workload presented by the clients by fully utilizing the resources available.
Transitional	is one of four categories used in the PSP program and EA to guide technology use in the State of Arizona (see also emerging, obsolescent, and strategic). “Transitional” implies that the State’s Enterprise Architecture promotes other standard technologies. Agencies may be using this technology as a transitional strategy in movement to a strategic technology. This technology may be waning in use or no longer supported.

Keyword	Description
Transmission Control Protocol (TCP)	is an OSI Layer 4 protocol. TCP is a connection-oriented transport layer protocol that provides reliable, full-duplex, data transmission.
Transport Layer Security (TLS)	is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer (SSL). TLS is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol provides connection security with some encryption method such as the Data Encryption Standard (DES). The TLS Record Protocol can also be used without encryption. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate an encryption algorithm and cryptographic keys before data is exchanged. The TLS protocol is based on Netscape's SSL 3.0 protocol; however, TLS and SSL are not interoperable. The TLS protocol does contain a mechanism that allows TLS implementation to revert to SSL 3.0.
Traversal Using Relay NAT (TURN)	is an IETF Internet Draft protocol that allows for an element behind a NAT or firewall to receive incoming data over TCP or UDP connections. It is most useful for elements behind symmetric NATs or firewalls that wish to be on the receiving end of a connection to a single peer. TURN does not allow users to run servers on well-known ports if they are behind a NAT; it supports the connection of a user behind a NAT to only a single peer. In that regard, its role is to provide the same security functions provided by symmetric NATs and firewalls, but to turn the tables so that the element on the inside can be on the receiving end, rather than the sending end, of a connection that is requested by the client.
Trusted platform	is a platform that can be trusted by local users and by remote entities. The trusted platform uses a behavioral definition of trust that an entity (an individual or information system that has access to an information system or to its data, records, or documents) can be trusted if it always behaves in the expected manner for the intended purpose. The basis for trusting a platform is a declaration by a known authority that a platform with a given identity can be trusted to measure and report the way it is operating.
Trusted-peer	is a participant in a community of interest.
Tuxedo	, which stands for “Transactions for UNIX, Enhanced for Distributed Operation,” is a middleware product that uses a message-based communications system to distribute applications across various operating system platforms and databases. Tuxedo operates as an extension of the operating system: as a platform for execution as well as development. It is designed for the creation and administration of e-commerce online transaction processing (OLTP) systems.
Two-tier client/server applications	, refer to Application Architecture Perspectives.
Unicast	is a method used to distribute information where packets are sent to a single network destination.
Unified Modeling Language (UML)	is a standard notation for the modeling of real-world objects as a first step in developing an object-oriented design methodology. UML is an accepted standard of the Object Management Group (OMG), which is also sponsoring CORBA as the industry standard for distributed object programming.

Keyword	Description
Uniform Driver Interface (UDI)	is designed to enable any given device to work across different platforms and operating environments, particularly across various implementations of the UNIX operating system. UDI results in a design architecture that provides standard interfaces to which device drivers can be written. UDI is the driver API specification of choice for non-intelligent I/O devices (that is, those that do not have an input/output processor), as well as for intelligent devices. It is also preferred for devices that stream their data.
Universal Description, Discovery, and Integration (UDDI)	are an XML-based registry for businesses worldwide to list themselves on the Internet. Its ultimate goal is to streamline online transactions by enabling companies to find one another on the Web and make their systems interoperable for e-commerce. The UDDI specification utilizes World Wide Web Consortium (W3C) and Internet Engineering Task Force (IETF) standards such as XML, HTTP, and Domain Name System (DNS) protocols. It has also adopted early versions of the proposed Simple Object Access Protocol (SOAP) messaging guidelines for cross-platform programming.
UNIX	was the first open or standard operating system that could be improved or enhanced by anyone. A composite of the C language and shell (user command) interfaces from different versions of UNIX were standardized under the auspices of the IEEE as the Portable Operating System Interface (POSIX). In turn, the POSIX interfaces were specified in the X/Open Programming Guide 4.2 (also known as the "Single UNIX Specification" and "UNIX 95"). Version 2 of the Single UNIX Specification is also known as UNIX 98. The Open Group, an industry standards organization, which certifies and brands UNIX implementations, now owns the “official” trademarked UNIX.
Unshielded Twisted Pair (UTP)	is a twisted-pair wire without the jacket shielding, used for short distances. It is subject to electrical noise and interference.
User	refers to an individual or group who has access to an information system or its data.
User Datagram Protocol (UDP)	ermits packets to be sent with a minimum of protocol overhead. UDP does not guarantee delivery since there is no checking for missing, out-of-sequence, or duplicate packets and no acknowledgements are sent.
UserID	is the most common form of electronic identification for internal access to an individual agency or the State’s applications, information, and resources. Each authorized user has an individual, unique identifier paired with a password used for authentication by knowledge.
Utility software	are programs that provide an addition to the capabilities provided by the device’s operating system. In some usages, a utility is a special and nonessential part of the operating system. A print utility, text editor, sort utility, data import utility are examples. Utilities are not absolutely required to run programs and, if not provided with the operating system, can usually be added.
Vendor costs	are the costs of all hardware, material, software, transportation, vendor support and all other identifiable costs associated with the vendor’s proposal or bid (ARS 41-2553).
Vendor Independent Messaging (VIM)	is an open API enabling developers to access proprietary Lotus mail services.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Vendor support	is the services provided by the vendor for items such as consulting, education, management of the information systems or telecommunication systems, system planning, system development, system integration, and maintenance (ARS 41-2553).
Versatility	is the ability of a software application or product (hardware or software) to be capable of, or adapted for, many uses, or applications.
Virtual Interface (VI)	architecture is a protocol standard that is designed to allow server-to-server communication with as little CPU use as possible. VI enables direct memory-to-memory transfer and allows for application access without tapping into the operating system. VI is transport independent and can be transported over Fiber Channel and Gigabit Ethernet. VI provides a shorter protocol stack. VI is mainly used in a “trusted peer” environment. It is optimized for data transfer in a controlled, high-speed, low-latency network.
Virtual Private Networks (VPN)	are network partitions of shared public network resources between multiple users to form a private network that appears private to users, but is still part of a larger public network.
Virtual Storage Access Method (VSAM)	is a file management system for primarily mainframe operating systems. Using VSAM, data records can be created and accessed in the sequential order that they were entered. VSAM can also save and access each record with a key. Software applications that access VSAM files are still supported in legacy applications.
Virus	is a piece of programming code written and buried within an existing program, to cause some unexpected and undesirable event, when the program is executed.
Virus, boot sector	are viruses that infect the first sector of a diskette or hard disk, which contains the master boot record, and are launched when a computer initializes with an infected disk. If a computer is booted with an infected diskette, the infected sector is loaded into memory and writes itself to the master boot sector on the hard drive. The virus stays in memory and infects new diskettes when the operating system accesses a new diskette and infects the boot sector of that disk. A boot sector virus, unlike other forms of viruses, does not travel across a network.
Virus, File Infector	is a type of virus that attaches itself to executable files, such as files with the extension .COM, .EXE, .DLL, .OVR, or .OVL. When the file is run, the virus, which operates in memory, spreads by attaching itself to other executable files. These types of viruses usually cause problems on LAN servers that run local applications shared by multiple systems. Unlike boot sector viruses, they can travel via a network as e-mail attachments or via file transfers. Gateway-based antivirus products stop the spread of these network-transported viruses by intercepting them at the network perimeter.
Virus, logic/time bomb	like a real bomb, a logic bomb will lie dormant until triggered by some event. The trigger may be a specific date, number of times executed, a random number, or a specific event such as a deletion or an addition of a specific record type. When triggered, it will usually do something damaging. This can range from changing data somewhere on a disk to making the entire disk unreadable. This is the most insidious attack; it causes damage before it is detected.

Keyword	Description
Virus, multipartite	is viruses that infect both boot sectors and executable files. They can combine some or all of the stealth techniques, along with polymorphism to prevent detection.
Virus, polymorphic	is viruses are encrypted viruses that change their appearance with each infection. They are difficult to detect because they hide from the antivirus software. In addition, these types of viruses complicate the AV software procedure because they alter the encryption algorithm with each infection.
Virus, stealth	are viruses that hide from both the operating system and antivirus software by residing in memory and intercepting attempts to use the operating system via system calls. The virus hides, from users and the antivirus software, the changes it makes to file size, directory structure, and/or other operating system aspects. Stealth viruses must be detected while they are in memory. Once found, they must be disabled in memory before the disk-based components can be corrected.
Virus, Trojan horses	are not really viruses because they do not propagate themselves. Rather, they attack specific computers by enticing unsuspecting users into executing a command that appears benign. These commands can include seemingly innocent activities, such as initiating a screen saver, accessing an e-mail attachment, or downloading executable files from an untrusted Web site, which can then execute commands to destroy problematic. When a file containing an infected macro is used, the infected file reproduces the virus into files or to give a hacker access to important system files. Although the Trojan horse does not inherently self-replicate, the introduction of and increase in use of Microsoft ActiveX control and Sun Java applet technology has increased the opportunity for Trojan horses to spread dramatically. Trojan horses can be used by hackers to enter the network and use Hypertext Transfer Protocol (HTTP) to establish communications with the stealth programmers.
Visual Basic® (VB)	is a programming environment in which a programmer uses a graphical user interface to choose and modify pre-selected sections of code written in the BASIC programming language. VB includes a rapid application development (RAD) tool for building object-oriented programming applications.
Visual FoxPro® (VFP)	is a tool for building database solutions from multi-tiered database applications, to data-intensive COM components, and XML Web services. Visual FoxPro is a Rapid Application Development (RAD) tool with full object orientation and integrated client server capabilities. Visual FoxPro® supports XML standards, such as SOAP and WSDL, as well as the creation of .NET Web services in the same environment. Along with full support for WindowsXP®, Visual FoxPro® XML support allows integration with .NET Enterprise Servers such as SQL Server 2000®. Visual FoxPro® still supports standard Xbase procedural programming with new extensions to the language provide the power and flexibility of object-oriented programming.
Voice over IP (VoIP)	is the capability to carry normal telephony-style voice over an IP-based Internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls, and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Voice Profile for Internet Mail (VPIM Version 2)	is currently a proposed Standard (IETF RFC 2421) Applicability Statement. It is an application of Internet Mail originally intended for sending voice messages between voice messaging systems. As such, VPIM imposes several restrictions on the message and transport to support the characteristics of voice messaging. Many voice mail vendors have implemented systems according to IETF RFC 2421 and are in the process of deploying these systems around the world. Most vendors have completed (or are currently involved in) interoperability testing of VPIM products and have posted their results on the VPIM website. VPIM Version 3 will support interoperability with deployed desktop email clients. A secondary goal is to specify interoperability with Version 2. The result is that the semantics of a voice or fax message within an email message can be interpreted at as many clients as possible. An initial proposal for VPIM v3 [also known as Internet Voice Mail (IVM)] is currently documented in several Internet Drafts: VPIM v3 Goals, VPIM v3 Unified Messaging (Primary Content), VPIM Addressing, and VPIM v3 Specification.
VoiceXML	is an application of the Extensible Markup Language (XML) which, when combined with voice recognition technology, enables interactive access to the Web through the telephone or a voice-driven browser. An individual session works through a combination of voice recognition and keypad entry.
Vulnerability scanner	detects and identifies security holes by probing for and confirming vulnerabilities.
Web services	(sometimes called application services) are services (usually including some combination of programming and data, but possibly including human resources as well) that are made available from a business's Web server for Web users or other Web-connected programs. Providers of Web services are generally known as application service providers.
Web Services Description Language (WSDL)	is an XML-based language used to describe the services a business offers and to provide a way for individuals and other businesses to access those services electronically. WSDL is the cornerstone of the Universal Description, Discovery, and Integration (UDDI) initiative.
Web Services for Remote Portals (WSRP)	standardizes the consumption of Web services in portal front ends, as well as the way in which content providers write Web services for portals.
Web Services User Interface (WSUI)	initiative is a vendor-neutral standard that enables application developers and sites to deliver entire applications over the Internet as Web services. WSUI was developed to provide a common language for delivering applications over the Web that can directly be embedded into e-business and portal sites. WSUI uses a simple schema for describing a WSUI "component" that calls backend SOAP and XML services and uses XSLT stylesheets to construct user-facing views to enable users to interact with the services. By adopting WSUI, vendors, customers, and developers gain the ability to dynamically share applications across web sites without being concerned with the backend implementation of service interfaces.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Web-Based Enterprise Management (WBEM)	is a set of management and Internet standard technologies developed to unify the management of enterprise computing environments. WBEM provides the ability for the industry to deliver a well-integrated set of standard-based management tools leveraging the emerging Web technologies. The DMTF has developed a core set of standards that make up WBEM, which includes a data model, the Common Information Model (CIM) standard; an encoding specification, xmlCIM Encoding Specification; and a transport mechanism, CIM Operations over HTTP.
Webmasters Group	is a forum, hosted by GITA, for the State's Webmasters. It provides an opportunity for Webmasters from all areas of state government to come together and exchange ideas, brainstorm new services and features, and see some of the latest technology offerings on the market today.
Weighted Fair Queuing (WFQ)	is a system of scheduling packets that are waiting for transmission that separates the packets into classes of different priorities and guarantees that each class receives some portion of the available bandwidth. WFQ dynamically adjusts bandwidth allocations based on the traffic parameters and the relative amounts of traffic, reducing jitter and producing more predictable round-trip delays.
Wide Area Network (WAN)	is a network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. A WAN typically consists of multiple LANs that are linked together. A WAN typically serves as a customized communication "backbone" that interconnects all of an organization's local area networks.
Will	identifies anticipated activities.
Wired-for-Management	is the Intel-led, industry-supported initiative to make Intel architecture-based systems universally manageable and universally managed without sacrificing agility or performance.
Wireless Application Environment (WAE)	provides the application-centric content presentation and programming interactions between WAP/web applications and wireless devices containing a micro-browser.
Wireless Application Protocol (WAP)	defines a layered protocol stack that contains a session protocol (WSP), a transaction protocol (WTP), a security protocol (WTLS), and a datagram protocol (WDP). This stack isolates the application from the bearer when used as a transport service.
Wireless Communication	is the ability to transmit data from point to point without the presence of a physical connection between the communicating devices. The key characteristic of wireless is the use of a multiple access radio system instead of wires to create the distribution/access network, whether or not point-to-point microwave is used as the backbone of the network.
Wireless Datagram Protocol (WDP)	is a general datagram service offering a consistent service to the upper layer protocols and communicating transparently over one of the available underlying wireless bearer services.
Wireless Markup Language (WML)	, formerly called Handheld Devices Markup Languages (HDML), is a language that allows the text portions of web pages to be presented on cellular telephones and personal digital assistants (PDAs) via wireless access.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
Wireless profiled (for a given IETF protocol)	consists of the detailed, normative references to standardize the use of the IETF protocol by wireless devices in the WAP.
Wireless Session Protocol (WSP)	provides ways to establish a session from client to server, agree on used protocol functionality, exchange content, and suspend and resume sessions. It provides both connection-mode session and non-confirmed, connectionless services. The core of the WSP is the HTTP v1.1 protocol and all the methods defined by the HTTP v1.1 are supported. When providing connection-mode, the WSP utilizes the Wireless Transaction Protocol layer. In the case of connectionless mode, the WSP takes advantage of the Wireless Datagram Protocol layer.
Wireless Transaction Protocol (WTP)	provides a lightweight, transaction-oriented protocol that reliably delivers requests from the client to the server and responses from the server back to the client. WTP runs on top of a datagram service and it is designed for interactive browsing.
Wireless Transport Layer Security (WTLS)	is the security level for Wireless Application Protocol (WAP) applications. Its primary goal is to provide privacy, data integrity, and authentication for WAP applications. Based on Transport Layer Security (TLS) v1.0 (a security layer used in the Internet, equivalent to Secure Socket Layer 3.1), WTLS was developed to address the problematic issues surrounding mobile network devices - such as limited processing power and memory capacity, and low bandwidth - and to provide adequate authentication, data integrity, and privacy protection mechanisms.
Wire-speed	is whatever rate of data transfer a given telecommunication technology provides at the physical wire level. Wire-speed, an adjective, describes any hardware device or function that tends to support this data transfer rate without slowing it down. It is common to refer to functions embedded in microchips rather than in software programming as working at wire speed. Switches,, routers, and other devices are sometimes described by their manufacturers as operating at wire speed.
WordPerfect® Office	is a productivity software suite that includes word processing (WordPerfect®), spreadsheet (Quattro® Pro), presentation, an e-mail client and address book, database, and speech-recognition software.
Workstation	is a terminal or personal computer attached to a local area network (LAN) or a mainframe network that in turn shares the resources of one or more large computers.
World Wide Web Consortium (W3C)	is an industry consortium that seeks to promote standards for the evolution of the Web and interoperability between WWW products by producing specifications and reference software. Although industrial members fund W3C, it is vendor-neutral, and its products are freely available to all. The Consortium is international, jointly hosted by the MIT Laboratory for Computer Science in the United States and in Europe by the French National Institute for Research in Computer Science and Control (INRIA) who provide both local support and perform core development.
Worm	is a type of malicious code that does not alter files like a virus but resides in a computer's memory and replicates itself throughout a network (including the Internet) without the user being aware. It consumes system resources and floods the network with excessive traffic, eventually overloading the system and disrupting service.

Keyword	Description
WS-Coordination	is a proposed IT industry standard for how individual Web services can interact in order to accomplish an application task. The WS-Coordination interface defines a context within which coordination is to take place and the specific items of data that are to be exchanged in order for transactions to complete successfully as part of an overall business process defined in a Business Process Execution Language (BPEL) program. WS-Transaction is a companion specification for what will constitute the completion of a transaction
WS-Security	is a proposed IT industry standard that addresses security when data is exchanged as part of a web service. WS-Security is one of a series of specifications from an industry group. Related specifications include the Business Process Execution Language (BPEL), WS-Coordination, and WS-Transaction. WS-Security specifies enhancements to SOAP (Simple Object Access Protocol) messaging aimed at protecting the integrity and confidentiality of a message and authenticating the sender. WS-Security also specifies how to associate a security token with a message, without specifying what kind of token is to be used. It does describe how to encode X.509 certificates and Kerberos tickets. In general, WS-Security is intended to be extensible so that new security mechanisms can be used in the future.
WS-Transaction	is one of a series of proposed specifications that define what constitutes a transaction and what will determine when it has completed successfully. Each transaction is part of an overall set of activities that constitute a business process that is performed by cooperating Web services. The overall business process is formally described using the Business Process Execution Language (BPEL). WS-Coordination is a companion specification that defines the context and method for information exchange during the business process.
WYLBUR	is an interactive terminal system, and many important applications may still depend on it. However, computing directions and trends make it apparent that WYLBUR will not remain a viable system for the long-term future.
X Window Systems	is a distributed, network-transparent, device-independent, multitasking windowing, and graphics system originally developed by MIT for communication between X terminals and UNIX workstations. X terminals allow a user simultaneous access to several different applications and resources in a multi-vendor environment through implementation of X Windows.
X.25	is the CCITT protocol standard for connecting to packet-switched networks. Typically used to connect wide area networks, packet switching breaks network data into smaller packets and sends the packets from point to point through interconnected switches.
X.500	is an overall model for Directory Services in the OSI world. The model encompasses the overall namespace and the protocol for querying and updating it. The protocol is known as "DAP" (Directory Access Protocol). DAP executes over the full OSI network protocol stack.
X.509/PKIX	refers to the collective efforts of the X.509 workgroup and the IETF workgroup building on the X.509 effort to create PIX. These workgroups provide the technical standards as well as the basic operational framework (PKIX) forming a basis for relating the various roles in any use of PKI.

Policies, Standards, and Procedures (PSP) and Enterprise Architecture (EA) Glossary of Terms

Keyword	Description
X/Open	was an international consortium of vendors who were defining a common application environment to provide applications portability. X/Open is now part of The Open Group.
XML for Analysis (XMLA)	specification is an open, industry-standard, web service interface designed specifically for online analytical processing (OLAP) and data-mining functions. XML for Analysis is a Simple Object Access Protocol (SOAP)-based XML API, designed specifically for standardizing the data access interaction between a client application and a data provider working over the Web. Under traditional data access techniques, such as OLE DB and ODBC, a client component that is tightly coupled to the data provider server must be installed on the client machine in order for an application to be able to access data from a data provider. Tightly coupled client components can create dependencies on a specific hardware platform, a specific operating system, a specific interface model, a specific programming language, and a specific match between versions of client and server components. The requirement to install client components and the dependencies associated with tightly coupled architectures are unsuitable for the loosely coupled, stateless, cross-platform, and language independent environment of the Internet. To provide reliable data access to web applications, the Internet, mobile devices, and cross-platform desktops need a standard methodology that does not require component downloads to the client. The specification is built upon the open, Internet standards of HTTP, XML, and SOAP, and is not bound to any specific language or technology.
XQuery	is a query language that uses the structure of XM. XQuery can express queries across different of data, whether physically stored in XML or viewed as XML via middleware. The XQuery specification describes a query language called XQuery, which is designed to be broadly applicable across many types of XML data sources. XML is a versatile markup language, capable of labeling the information content of diverse data sources including structured and semi-structured documents, relational databases, and object repositories.